PUBLIC-PRIVATE PARTNERSHIPS: A TOOL FOR ENHANCING CYBERSECURITY

by
Jake Rogers

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August 2016

Abstract

The development of cyber technologies has altered the way in which interactions occur on a daily basis at the individual, local, national, and international levels. Cyberspace has provided a myriad of outreach capabilities for people to access information and connect with others around the world. Information accessibility, education, social services, economic trading, communication, politics, diplomacy, and just about every function and form of interaction now occurs through this cyberspace or related cyber technologies. Both the public and private sectors are heavily dependent upon cyberspace. However, the rapid growth of this new domain has altered security issues in the world. Potential use of this domain to commit crimes or acts of ill-nature creates a viable threat. Cyber threats are imminent and crimes are instantaneous, therefore creating the need for enhancing cybersecurity in both sectors. But how can this be achieved?

The development of public-private partnerships can be a major tool for the enhancement of cybersecurity. The following chapters focus on the specific details and development of these partnerships. This occurs through the discussion on the characteristics and effective functions of these partnerships with application to cyber scenarios. This also includes relevant case studies of cyber public-private partnerships. Furthermore, some of the legal challenges inhibiting the development of public-private partnerships on a global scale, are also examined. The adaption of public-private partnerships can be a viable, successful tool to develop collaboration between the public and private sectors. The collaboration between both sectors will be necessary in order to combat growing cybercrimes and threats in today's world. The instantaneous and far

reaching threats and security concerns in the cyber world present a difficult task for individuals, state, and non-state actors. Without the development of these public-private partnerships the security concerns of cyberspace may present an insurmountable challenge, however, the adaption of these partnerships can enable the development of a strong cybersecurity structure that can combat and respond to threats in real time.

Thesis Advisors and Readers

Dr. Mark Stout, Dr. Sarah O'Byrne, Dr. Dorothea Wolfson, Dr. Alexander Rosenthal, Dr. Bryan Gibson, Dr. Michael Warner, and Rhea Siers.

Preface

This thesis is the culmination of the Master of Arts in Global Security Studies. The research has been originally formulated and the findings and arguments are of an independent nature. I would like to acknowledge all of the staff of the Johns Hopkins University, Advanced Academic Programs, family, and friends, who have aided me in this process. This includes Dr. Mark Stout, Dr. Sarah O'Byrne, Dr. Dorothea Wolfson, Dr. Alexander Rosenthal, Dr. Bryan Gibson, and all of the others who have provided me with assistance along this journey.

Table of Contents

List of Figures

Introduction

The world is rapidly changing. Security issues used to be more concrete with known state and non-state actors on the international field. Threats and events occurred based on known players during daily interactions and conflicts. The world continued this way for years until the revolution of information technology. The onset of the last decade has brought about a major change in the domain in which the world interacts. Individuals, state, and non-state actors currently use cyberspace as its main line of world interaction. This domain is completely digital with instantaneous data transfer across international borders. Social, political, economic, and almost all types of data and communication now occur through cyberspace. In addition, digital communications are vital for national and international military and civilian systems to provide health services, communication, assistance, and many other important necessities of the world. Cyberspace has tremendous upside.

However, not every actor using cyberspace has positive intentions. Many use digital networks as a means to commit cybercrimes, which can range from theft to warfare. Therefore, cybersecurity has become a major priority of both the public and private sectors. The need for strong cybersecurity systems is crucial as threats and crimes are imminent and can occur from anywhere in the world. This is the first domain of interaction in which stronger capabilities does not always equate to strong security. Cyber and information technology is asymmetrical. One person or a small group can now have an impact on major world entities in both the public and private sectors. In some cases, cybercriminals can have an impact on major policy decisions and the safety and security

of everyday citizens. The applications of the cyber world are truly incredible, however, this makes everyone vulnerable.

Furthermore, scholars have developed very little theory on cybercrimes as they are new to the international field. Cybersecurity lacks an effective framework for developing partnerships, writing laws, effectively sharing information, protecting personal liberties, and overcoming many challenges. It has been difficult to determine what is the best method to combat these cybercrimes. Cybersecurity requires instantaneous response from multiple entities within both the public and private sectors.

This thesis calls for the development of cyber public-private partnerships in order to increase prevention and detection of cybercrimes as well as decrease response time to real threats and crimes at multilateral levels of the public and private sector. Chapter one will discuss the effectiveness of public-private partnerships for enhancing cybersecurity. This will be accomplished through the collaboration of both the public and private sectors in order to increase prevention and detection and decrease response time to cybercrimes. This idea will be supported, in part, by the Intelligence and National Security Alliance's paper "Addressing Cyber Security Through Public-Private Partnerships."[1] Chapter two will discuss case studies of various multinational private companies as well as public agencies in order to analyze the effective functions of cyber public-private partnerships. This notion will be supported by the Center for Democracy and Technology's paper "Improving our Nation's Cyber security through the Public-Private Partnership."[2]

---

[1] "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models", Intelligence and National Security Alliance, November 2009. http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

[2] "Improving our Nation's Cybersecurity through the public-private partnership", Center for Democracy and Technology, March 8th, 2011. https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf

Chapter three will discuss some of the limitations inhibiting the development of cyber public-private partnerships. These ideas will be reinforced by Judith Germano, professor at the NYU School of Law and Fellow at the Center on Law and Security, in her piece entitled "Cybersecurity Partnerships: A New Era of Public-Private Collaboration."[3] Taken together, this thesis argues that the public and private sectors must work together to successfully combat cybercrime on an international level.

[3] Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014.
http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

Chapter One

The World Today: A Brief Overview

The past century primarily consisted of known threats from world powers. Security issues were identifiable and the timeframe of these issues were, comparatively, slow to develop, thus, allowing for an appropriate diplomatic response. However, the advent of the 21st century has brought on a new set of challenges. The world has experienced a rise of international players with significant influence on world events. Governments, non-governmental organizations, international organizations, terrorist groups, companies, certain officials, the media, and many other participants play a significant role in international events and decisions worldwide. Political, economic, social, military, environmental, and a broad array of issues persist in the world today, but one major technological change and expansion has shifted the scope and severity of these issues.

The rapid growth of the cyberspace (commonly referred to as the Internet) and its accessibility worldwide have completely altered security issues and world policy. Cyberspace is a new digital network in which people, groups, organizations, and governments are now connected instantaneously. Cyberspace has allowed for the world to be interconnected in a new way. In addition, cyberspace changes rapidly, as each individual changes the domain every time it is accessed. This new network has provided many tremendous outreach capabilities for people to access information and connect with others around the world. Information accessibility, education, social services, economic trading, communication, politics, diplomacy, and the list goes on and on of areas and services that have benefitted from the growth of cyberspace.

Unfortunately, the growth of cyberspace has led to the use of this network for negative and criminal purposes.[4] Cybercrimes are occurring at an ever-increasing rate. These crimes put people, groups, organizations, companies, and governments at risk as information security is threatened. Potential use of cyber networks for warfare and cybercrimes has led to the rise of cybersecurity as a growing field and industry. However, because of the instantaneous nature of cybercrimes and the instant threat capability, responses and identification of these crimes are slow and sometimes unsuccessful. Governments, companies, organizations, and other groups must develop a rapid, coherent response to combat the threats of these cybercrimes. In addition, it is usually the duty of the federal government to develop national security. But in cyberspace both the public and private sector are vulnerable, thus, calling for the joint effort of both sectors.

President Obama acknowledged the threat of cybercrimes in a speech at Stanford University. He said, "These cyber threats are a challenge to our national security. Much of our critical infrastructure —our financial systems, our power grid, health systems—run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before. Foreign governments and criminals are probing these systems every single day."[5] In addition, other countries and alliances are recognizing the significance of cybersecurity. The NATO web page "Cyber defense is part of NATO's core task of collective defense" discusses the

[4] Kristen Finklea and Catherine Theohary, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement". CRS Report R42547. January 15th, 2015. https://www.fas.org/sgp/crs/misc/R42547.pdf

[5] President Barack Obama, "Remarks by the President at the Cybersecurity and Consumer Protection Summit", Cybersecurity and Consumer Protection Summit, Stanford University, February. 13, 2015. https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

importance of cybersecurity in the world today.[6] There must be a joint effort to meet new challenges that cyberspace brings about.

But how should this joint effort be achieved? What is the best way to defend against cyber-attacks? Experts have increased cyber defense and networks with firewalls, developed programs to track hackers, and used a broad array of other tactics. There are some strategies in place, but there still has been a lack of effectiveness. This is evident from hacks against Sony, Office of Personnel Management (OPM), and other major networks. OPM was hacked in 2015, leading to the release of a large amount of sensitive and classified information.[7] In addition, in 2015, Iran's revolutionary guard hacked email and social media accounts of Obama Administration officials.[8] It can be stated that there is no shortage of cybersecurity issues developing worldwide.

Therefore, the focus of this paper will be on the development of Public-Private Partnerships (PPPs) as an effective means of combating the growing threats of cybercrime in our world today. The use of PPPs will be crucial to defend against cybercrimes and must become an integral part of world strategy. The following sections will discuss cybersecurity, the use of PPPs, as well as their elements and effectiveness, past and current examples, and an outlook to the future, and will analyze books, reports, media, government agencies, and other sources to provide comprehensive evidence of

---

[6] "NATO Cyber Defence", Accessed November 7th, 2015 http://www.nato.int/cps/en/natohq/topics_78170.htm

[7] Nakashima, Ellen, "Hacks of OPM databases compromised 22.1 million people, federal authorities say", *Washington Post,* July 9th 2015, Accessed November 8th, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say

[8] Jay Solomon, "U.S. Detects Flurry of Iranian Hacking", *The Wall Street Journal*, November 4th 2015, Accessed November 10th, 2015. http://www.wsj.com/articles/u-s-detects-flurry-of-iranian-hacking-1446684754

these topics. As we have learned from the past, threats will always exist, thus, it's imperative to use PPPs as a method of countering the growing threats related to cyberspace.

Literature Review

There has been a significant amount of discussion on the possibility of a cyberwar. The literature on the concept of a cyberwar or conflict in cyberspace falls into three main groups. The first group argues that a cyberwar will not occur. The second group claims that a cyberwar has already occurred. The third group suggests that a cyberwar will occur. The following section will discuss these three groups.

The first group argues that a cyberwar will not occur. The conflicts that may develop in cyberspace will not lead to, or will not be considered, a war. Thomas Rid discusses this notion in his paper, entitled "Cyber War Will Not Take Place". Rid takes Clausewitz's definition of war and discusses that there has to be three major elements to constitute the concept of war. These include an act that is: violent in nature, is instrumental (has a means to an end), and is political in nature.[9] Rid argues that an act in cyberspace is likely to be too complex and convoluted to actually cause a violent conflict. He wrote, "in an act of cyber war, the actual use of force is likely to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties."[10] In other words, a conflict or attack in cyberspace is unlikely to have all three attributes, and, therefore, will not be considered a cyberwar. Rid classifies cyberattacks and events under the categories of sabotage, espionage, or subversion.[11]

---

[9] Thomas Rid. *Cyber War Will Not Take Place*. Journal of Strategic Studies, Vol. 35 No. 1 (February 2012). p. 8.

[10] Ibid. Thomas Rid. *Cyber War Will Not Take Place*. p. 9.

[11] Ibid. Thomas Rid. *Cyber War Will Not Take Place*. p. 15.

These actions are primarily used to extract information, weaken systems, and undermine authority. According to this group, a cyberwar will not occur because cybercrimes and attack will not amount to a violent conflict that is instrumental and political in nature.

However, others share a different viewpoint. The second group claims that a cyberwar has already occurred. Recent events have already amounted to a cyberwar. Robert Clarke and Robert Knake in their book, Cyber War, discuss events that could already be considered acts of cyberwar. The authors cite examples from conflicts between Israel and Syria and the United States and Iraq in the 1990's in order to articulate their argument. Israeli spies "tricked" the Syrian Defense Network and the United States Central Command sent emails to Iraqi officers to lay down their arms.[12] These acts constitute a cyberwar according to these authors. They wrote, "cyber war has begun. In anticipation of hostilities, nations are already 'preparing the battlefield.' They are hacking into each other's networks and infrastructures, laying in trapdoors and logic bombs – now, and in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability."[13] In essence, cyberwar has occurred and will continue to do so based on the ongoing nature and actions of state actors in cyberspace.

The third group suggests that a cyberwar will occur in the future. Cyber conflicts have occurred, but have not yet amounted to a war. This could entail anything from a small conflict to a large scale cyberattack. The attacks could occur on any vulnerable digital systems. In addition, military and civilian systems are susceptible to cyberattacks on these electronic networks. This idea is discussed by John Arquilla and David Ronfeldt

[12] Richard Clarke and Robert Knake. *Cyber war*. HarperCollins, 2011. p. 12.
[13] Ibid. Richard Clarke and Robert Knake. *Cyber war*. p. 21.

in their chapter, entitled "Cyberwar Is Coming", as part of their paper, *In Athena's Camp.* The authors wrote, "the information revolution will cause shifts both in how societies may come into conflict, and how their armed forces may wage war."[14] This idea is alarming as the future of international conflict is changing. The authors' overall argument is that netwar (warfare on civilian systems) and cyberwar (warfare on military systems) are imminent and will become the mode of conflict in the future.[15]

Similarly, John Stone in his article "Cyber War Will Take Place!" discusses the notion of a cyber conflict. He wrote, "my purpose here is to demonstrate that cyber war could take place."[16] Stone focuses his article on theorizing about the elements that could constitute conflicts as an act of cyber warfare. Cyberspace makes state and non-state actors exposed to threats from all types of enemies. Most of the literature focuses on imminent occurrence of a cyberwar and what elements would make up this conflict. It seems that a cyberwar will occur, if it has not already.

However, there is less literature on strategic solutions to defending civilian and military cyber systems. It appears likely that a cyberwar or conflict will occur. But the issue has become what is the best solution to respond? Responding includes preemptive defense and response after an attack. This chapter will offer a solution to this issue, in hopes, of filling a gap in the existing literature.

---

[14] John Arquilla and David Ronfeldt, "Cyberwar is Coming", *In Athena's Camp,* Rand Corporation, 1997, p.25

[15] Ibid. John Arquilla and David Ronfeldt, "Cyberwar is Coming", p. 33

[16] Stone, John, "Cyber War Will Take Place!", *Journal of Strategic Studies*, Vol.36, No.1, pp. 101-108, November 29th, 2012.

Public-Private Partnerships an Overview

First it is necessary to give a brief overview of PPPs as well as offer how this analysis is defining and using the term. Thus, this section will have two facets. The first facet is the definition and general description of a PPP, and characteristics of successful PPPs. The second facet will briefly explain the important distinction of PPPs as national, regional and international variations causing distinctions and differences under the broad category of PPPs.

A Public-Private Partnership is defined as an agreement between a private party and a government entity to offer a public service or asset. This definition stemmed from Public-private Partnerships: Theory and Practice in International Perspectives by Stephen Osborne.[17] The book describes the theory and practical applications of PPPs on a general scale across many industries. The PPP agreement is key as it links the public and private sectors, which in turn mitigates the risk of public services to private entities and promotes efficiency and productivity for certain ventures. The joint effort between a company and a government, a non-governmental organization and a government or any combination of public and private entities is the key factor that identifies a PPP. This is an important baseline to keep in mind as the arguments develop and to maintain focus on PPPs.

The next pieces to identify are factors that make a PPP successful. This is vital because PPPs in cybersecurity must have some of these characteristics in order to combat cyber threats. Mary Beth Corrigan, in her book Ten Principles for Successful Public/Private Partnerships, outlines ten characteristics of successful PPPs. These include: prepare properly for public/private partnerships; create a shared vision;

[17] Stephen P. Osborne, *Public-Private Partnerships: Theory and Practice In International Perspective.* London: Routledge, 2000 (Contents/Introduction).

understand your partners and key players; be clear on the risks and rewards for all parties; establish a clear and rational decision-making process; make sure all parties do their homework; secure consistent and coordinated leadership; communicate early and often; negotiate a fair deal structure; and build trust as a core value.[18] These ten characteristics are not always necessary, however, they are a beneficial outline to describe a strong, general foundation for PPPs.

The second facet to make note of, in this section, is that PPPs differ in legality, establishment, economic procurement, political use, and other variables. This distinction is important to recognize because PPPs that cross borders or even states within countries sometimes struggle to establish and function if these variables are neglected. The Brookings Institution released a report discussing differences between PPPs within the Transportation realm. "Countries and subnational governments around the world have been developing institutional structures for the promotion, development, and management of PPPs for several decades. None are precisely alike and they serve different functions depending on the needs, cultures, and traditions of the nations in which they operate."[19] The report acknowledges that PPPs differ in definition, function, policy formulation and coordination, quality control and technical assistance.

For example, Canada established its transportation PPP system as a corporation, while Australia has more of a federalist system for PPPs. To elaborate further when it comes to procurement, Canadian PPPs are allowed to apply for funding and provided

---

[18] Mary Beth Corrigan, *Ten Principles for Successful Public/private Partnerships,* Washington, D.C.: Urban Land Institute, 2005 (Contents/Introduction).

[19] Istrate, Emilia and Puentes, Robert. "Moving Forward on Public-Private Partnerships: U.S. and International Experience with PPP Units" BROOKINGS-ROCKEFELLER | PROJECT ON STATE AND METROPOLITAN INNOVATION | December 2011, pp. 6-7 http://www.brookings.edu/~/media/research/files/papers/2011/12/08-transportation-istrate-puentes/1208_transportation_istrate_puentes.pdf

such funding based on a merit and necessity system, however, in Australia PPPs must go through a procurement analysis on a sub-national basis before discussions with the federal government. Furthermore, laws vary as well between PPPs in countries. The United States has strong federal legislation for PPPs at the national level, but lacks coordination and similarities among state laws regarding PPPs.[20] Lastly, non-governmental organizations, companies, governments, and groups all have different rules and laws regarding matters related to engaging in PPPs. Therefore, it is vital to recognize these differences in order to work through limitations due to differences at sub-national, national, and international levels across multiple areas.

Definition of Terms Surrounding the Cyber Domain

Before delving into the main discussion, it is crucial to define certain terms that will appear throughout the paper. Some of these terms overlap and are technical therefore it is important to list and define these terms. Most of the definitions have come from the Department of Homeland Security (DHS) "glossary on common cyber terminology"[21] (Except for Cybercrime/ All other definitions under footnote 16/Also cited in Glossary). These terms are vital to understand beyond their technicalities because common terms in the context of cyberspace may have specific meanings or expanded meanings beyond the scope of their original definitions.

A few terms that are especially important to understand are cybersecurity, cyber threat, cyberspace, and cybercrime. This paper will define cybersecurity as "the activity

[20] Ibid. Istrate, Emilia and Puentes, Robert. "Moving Forward on Public Private Partnerships: U.S. and International Experience with PPP Units", pp. 10-13

[21] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, Feburary10th, 2015, Accessed November 10th, 2015. https://definedterm.com/a/download/document/11128

or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[22] Cyber threat will be defined as a "circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society."[23] Cyberspace will be defined as "the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[24] Cybercrimes will be defined as criminal offenses committed via the Internet or otherwise aided by various forms of computer technology.[25] These actions include terrorism, hacking, theft, unauthorized access, information dissemination, fraud, scams, copyright of code, and many other crimes that exist on computer, smartphone, or any digital network. Readers may refer to the appendix for a glossary of other terms.

Public-Private Partnerships: technicalities, effectiveness, purposes, and advantages

As stated previously, PPPs are an agreement between a private party and a government entity to offer a public service or asset.[26] (Figure 1.1/Appendix 1) But how do PPPs function, technically speaking? What is the purpose of PPPs? What is the

[22] Ibid. *Explore Terms: A Glossary of Common Cybersecurity Terminology,* Accessed November 10th, 2015.
[23] Ibid. *Explore Terms: A Glossary of Common Cybersecurity Terminology,* Accessed November 10th, 2015.
[24] Ibid. *Explore Terms: A Glossary of Common Cybersecurity Terminology,* Accessed November 10th, 2015.
[25] *Cybercrimes,* FindLaw, Accessed November 10th, 2015 http://criminal.findlaw.com/criminal-charges/cyber-crimes.html
[26] Ibid. Stephen P. Osborne, *Public-Private Partnerships: Theory and Practice In International Perspective* (Contents/Introduction).

process of developing a PPP? What are the advantages that make PPPs effective? This section will discuss the technicalities, purposes, advantages, and effectiveness of utilizing PPPs.

The purpose of a PPP is to link the public and private sectors to increase efficiency and productivity. For the most part there are two fundamental purposes for PPPs. The first is that the private sector can bring expertise and efficiency to the public sector, in order to deliver "facilities and services traditionally procured and delivered by the public sector."[27] This creates efficiency and allows both sectors to function with less limitation in order to provide a public good or service. The second purpose of the PPP arrangement is to ensure that borrowing occurs by the private partner of the agreement. This ensures that the public sector has minimal to no risk in partaking in this agreement. In addition, a PPP is an "off-balance sheet" means of providing a public good or service without having to finance or document the PPP as their own agenda.[28] These fundamental purposes enable the PPP agreement to be a successful tool in order to achieve public sector objectives, while reducing risk, increasing efficiency, and stimulating the private sector. PPPs are a creative way of achieving joint cooperation and collaboration, in which both sectors benefit and share success, which is not easy to achieve in today's world.

The next important piece of the puzzle is the process of procuring and developing a PPP. There are generally six steps to the development process of a PPP[29]:

1) The Bidding Process: This is usually the first step in development of a PPP. The

[27] Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", Advocates for International Development, June 2012, Page 1
http://www.a4id.org/sites/default/files/files/[A4ID]%20Public-Private%20Partnership.pdf
[28] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", P.1
[29] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", pp 1-3

public sector, usually the government, finds a need to deliver a public good or service; thus, they advertise and reach out to private groups. These private groups then "bid" for the project and the group that is selected is awarded a concession.

2) Project Company: Usually, the private entity will enter into a contract with the public sector and begin to raise funds for the project. Sometimes, a new private company, or a multitude of private companies, will be procured in order to provide special purpose vehicles (SPVs). This disseminates the risk among many investors.
3) Sponsors: These sponsors will monitor the activities surrounding the project. The PPP will contract these sponsors. The sponsors become the principal shareholders with the most at stake.
4) Documentation: The sponsors will work with the private sector to develop the legal framework and documentation in order to ensure that the PPP meets the legal requirements of local, national, federal, and international laws. This piece is key to ensure the legality of the PPP.
5) Funding: PPPs require initial liquid funding as well as long-term investments and loans that will secure the project. The funding process is slow and can come from the public and private sectors.
6) Implementation and Review of the PPP: The last step is implementing the PPP and executing the intentions of the PPP. As the PPP functions and delivers a project, asset, or service, a review process then observes and analyzes the success and failures of this PPP. This step allows for any adjustments to be made and oversight to be carried out.

These six steps are generally the process for developing a PPP. Figure 1.2 (Appendix 1) provides a real world example of a construction PPP.[30] The public entity finds a project company, who in turn, finds sponsors. The documentation and funding through direct agreements and other contractors provide the long-term security of loans for the project.

These drawn out processes of forming PPPs and the liabilities that come with doing so raise the question of what are the advantages of them? These main advantages are that PPPs are effective and worthwhile as a means of increasing efficiency and productivity. There are generally seven advantages to PPPs.[31]

1) PPP's have the best value for delivering a public good or service. The time and cost is efficiently used and monitored under a PPP agreement. This fact is definitely the most significant feature of a PPP. The baseline factor in operations is providing the best value for delivering an outcome while maintaining the most efficient manner in which to do so. PPPs apply the private sector principle of cost and time efficiency to deliver public goods or services, which are necessary in today's world.
2) Investments tend to be long-term, which establishes benefits over a long period of time. The long-term investment strategy allows the PPP to benefit people for a long period of time, thus, expanding the public goods or services. Resources are distributed as needed and monitored in order to ensure proper use and reduce waste.

[30] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", p.4
[31] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", p.4

3) The collaboration among the public and private sector is key in order to promote efficiency and use expertise to develop innovation. Collaboration is the fastest way to achieve outcomes and pool resources. With all of the security issues today, the public and private sectors fear that collaboration may lead to unauthorized exposure of information. However, without collaboration, innovation and inception of these vital PPPs the process of delivering goods or services is slowed.
4) There is a greater capacity for resources over the long-term. This piece is simple. The more resources available lead to a better chance of success for a PPP. This increases the amount of public goods and services that are available.
5) Public sector payments and funds are directly linked to incentives and success, thus, ensuring the use of taxpayer funds for good purposes. PPPs work against the issue of inefficient use of funds and resources.
6) The competitive market for private sector bids stimulates economic growth and connects economic success between the public and private sectors. Competition drives economic success for the markets. PPPs stimulate both public and private markets by constantly creating investments on both sides that transfer across the barriers between the markets.
7) PPPs are not subject to political interference. PPPs can operate without scrutiny and interjection of the public sector. This advantage is crucial in the delivery of public goods and services. This is probably the second most significant feature of a PPP, especially in democratic countries. Democracy is

inefficient for achieving directives. Therefore, PPPs deliver public goods and services but because they are operated by private entities, the PPPs can function more efficiently. The lack of political interference increases the effectiveness of PPPs.

For these listed reasons, PPPs are generally effective as a means of achieving public sector objectives through the use of private entities. PPP's efficiently allocate risk among private entities, as well as use the best knowledge and resources. "Clearly, effective public-private partnerships can be useful in fostering better working relationships and enhancing the business of government."[32] The reader should note that the effectiveness of a PPP makes it an instrumental tool in order to promote efficiency. This will be crucial as we apply the general principles of PPPs to the discussion of cybersecurity and the development of PPPs in that industry.

Effectiveness of Public-Private Partnerships for Cybersecurity

Cyberspace activities occur in real time. Activities happen instantaneously whether these activities have positive or negative effects. Thus, requiring a more rapid and coherent response. For example, a hacker uses a virus, spyware, spam, phishing, or any method to breach the firewall of a network and steals sensitive information from an unauthorized network without the necessary authentication. This was evident in the OPM, Sony, and Iranian hacks as previously mentioned. The issue is that response time to these attacks is slow in cyberspace. A private entity has to call the government and

[32] "Keys to Collaboration: Building Effective Public-Private Partnerships", The National Association of State Chief Information Officers (NASCIO) Corporate Leadership Council (CLC) Transforming Government: Role of Information Technology, May 2006, p.10 http://www.nascio.org/publications/documents/nascio-keys%20to%20collaboration.pdf

describe the attack, code, information stolen, and threats, etc. The government then has to alert all of its agencies: The Central Intelligence Agency (CIA), National Security Agency (NSA), Federal Bureau of Investigations (FBI), DHS, Intelligence Task Force, and all of the other agencies which have sensitive information. The process takes too much time for response, because as the first hack is dealt with, other hacks are already taking place.

Kim-Kwang Raymond Choo, an information security expert stated the problem perfectly when he said, "Increased variety and volume of attacks is inevitable given the desire of financially and criminally-motivated actors to obtain personal and confidential information."[33] The issue is so prevalent that Congress pushed the Cybersecurity Information Sharing Act of 2015, through the legislative process in a short timeframe. The Act has the mandate to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats."[34] Therefore, a beneficial method of dealing with this response issue would be the use of PPPs. PPPs are new to cyberspace, but if developed, can be an immensely useful tool to increase cybersecurity and defend and identify cybercrimes.

PPPs in cyberspace would be an effective tool against these cybercrimes. The key to this is the element of collaboration and cooperation. PPP's provide an avenue for the private and public sectors to work together to enhance cybersecurity. The idea of a PPP in cybersecurity promotes the public benefit of safer networks with increased awareness of

---

[33] Choo, Kim-Kwang Raymond, "The Cyber Threat Landscape: Challenges and Future Research Directions", ScienceDirect: Computers and Security, August 16th 2011, Accessed, 30 Sept. 2015. p.1 http://130.18.86.27/faculty/warkentin/SecurityPapers/Newer/Choo2011_C&S30_CyberThreatOverview.pdf

[34] Senate, *Cybersecurity Information Sharing Act 2015*. 114th Congress, 1st session, 2015, S.754, Accessed November 7th, 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754/text

threats, as well as methods of communication to prevent cybercrimes on a broad scale. PPP's also provide adaptability for the system to transform and react in real-time to threats whether from an individual, a terrorist group, a country, or anyone else. The White House in its National Security Strategy of 2015 called for the need for cooperation in regards to security networks. "The increasing interdependence of the global economy and rapid pace of technological change are linking individuals, groups, and governments in unprecedented ways. This enables and incentivizes new forms of cooperation to establish dynamic security networks, expand international trade and investment, and transform global communications. It also creates shared vulnerabilities, as interconnected systems and sectors are susceptible to the threats of climate change, malicious cyber activity, pandemic diseases, and transnational terrorism and crime."[35] Collaboration through PPPs will be a key method to thwart cybercrimes.

The Intelligence and National Security Alliance (INSA) released a report in which it discussed Cybersecurity through the PPP model. The report said, "The internet is a critical infrastructure necessary to the functioning of commerce, government and personal communication and national security. This system is not secure. Since the nation's cyber infrastructure is not government owned, a partnership of government, corporate and private stakeholders, is required to secure the Internet."[36] In cyberspace, the duty of national security, generally a public sector duty, has crossed the line into the private sector. Cyberspace is the first domain in which all parties and people are vulnerable to crimes; thus, PPPs are effective by efficiently utilizing available resources

[35] "National Security Strategy", White House, February 2015. pp. 15-16
https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf
[36]"Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models". Intelligence and National Security Alliance November 2009. p.3

to respond to these crimes and bolster security in order to provide a necessary public service. The report also highlighted the major components of a PPP for cyberspace. The groups involved were split into four categories.[37]

1) Telecommunications companies, software suppliers, Internet Service providers (ISP's).
2) The government as a regulator and partner in securing cyberspace (local, national, and international governments).
3) User groups: corporations, businesses, organizations, academia.
4) Users: Individuals who must share information.

The mission of the PPP would be "to establish reasonable standards and best practices such that anomalous activities and behaviors could be identified. This identification would then allow for notification (provided to users and suppliers alike) of the existence of these behaviors and vulnerabilities across processes and technology, enabling remedial action to minimize or prevent loss of assured access or privacy for users."[38] This mission summarizes three functions that make cyberspace PPPs effective.[39]

1) Detection- the partnerships identify and disseminate information on threat or agents of certain behaviors that present a concern.
2) Protection- the partnerships ensure compliance with standards and chastise those who do not comply.
3) Response- the partnership sets up a forum and framework for a coherent

[37] Ibid. "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models". Intelligence and National Security Alliance November 2009. p.6

[38] Ibid. "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models". Intelligence and National Security Alliance November 2009. p.8

[39] Ibid. "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models". Intelligence and National Security Alliance, November 2009. p.9

response to cybercrimes, data breaches, hacks, terrorism, etc. The response is coordinated among the public and private sectors; therefore, the crime gains widespread notoriety in an efficient manner.

These functions make a PPP effective for securing cyberspace. The following is the explanation of a general diagram (Figure 1.3/Appendix 1), which explains the basic process of how a cybersecurity PPP would function. A cybersecurity panel composed of individuals and experts from both sectors would oversee the partnership and create the necessary standard that partners must adhere to in their compliance. The panel would represent interests from both the public and private sectors. A government regulatory body reports to the panel to ensure the intentions of the public sector and to help oversee some of the other parties involved. This can create some friction; as private entities are not always willing to allow their information to be accessible to the government. Government officials on these panels ensure certain public rules that are usually specified in the contract when developing the PPP. These two bodies work in unison in order to[40]:

1) Regulate suppliers (Telecommunications companies, software suppliers, Internet Service providers (ISP's)) and users;
2) Inspect and enforce compliance from these suppliers and users;
3) Provide detection from threats and behaviors that jeopardize security;
4) Protect individual privacies and liberties of users and suppliers;
5) Respond to, and recover from, threats through information sharing, as represented in the arrows on the diagram (Figure 1.3/Appendix 1);

[40] "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models", Intelligence and National Security Alliance. pp. 9-11

6) Promote international collaboration with other organizations and countries in order to increase security and stop cybercrimes on broad scales; and

7) Promote US government collaboration and information sharing.

This structure of cyber PPPs, is key to its effectiveness. Cybercrimes can be identified and thwarted by the use of PPPs. The immense capabilities and flexibility to rapidly share information is the key basis of these PPPs.

Examples of Public Private Partnerships in Cybersecurity

To better understand how such collaboration works in PPPs this section will share a few examples. In addition, two companies will be discussed that focus on cybersecurity as a business model, helping companies protect their networks. This is crucial because in complement to the PPP it is also important to make note of private entities and their growth in the sector of cybersecurity.

The PPP in cyberspace that will be discussed was established primarily by the DHS. Information sharing became a crucial aspect of cybersecurity. The DHS along with other governmental agencies developed a massive PPP network for sharing information related to cybersecurity. These partners share information in order to protect critical infrastructure, power grids, communications services, secure information, and a vast variety of public goods, services, and information. The DHS website discusses the Information Sharing Analysis Centers (ISACs) which are centers that facilitate the information sharing process among the sectors.[41] The ISACs and the government agencies, along with a host of other sponsors (private entities) create a huge network of information sharing, thus, preventing cybercrimes on a broad scale with efficient and

[41] *Information Sharing,* Department of Homeland Security, Accessed November 10th 2015. https://www.dhs.gov/topic/cybersecurity-information-sharing

rapid responses. Figure 1.4 (Appendix 1) presents the diagram of this PPP network.[42] The diagram directly connects both the public and private sectors, while mitigating cost and risk to the private sectors. Let's take a further look at this PPP.

The White House, Department of Justice (DOJ), DHS, CIA, FBI, Department of Defense (DOD) and NSA represent the public sector on this diagram. The public sector has agencies that run within these departments on cybersecurity. These include the Cybersecurity and Communications (CS&C), the National Cybersecurity and Communications Integration Center (NCCIC), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Coordinating Center for Telecommunications (NCC), and many others. The DHS contracted the ISACs as their private entity or principle sponsor. The ISAC recruited other bodies in order to share the responsibility. These include the ISPs, businesses, individual users, and many others. The Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) coordinate these private entities and public agencies and report back to the entities and public sector.[43]

This PPP is one of the largest developed, which shows the growing concern in the field of cybersecurity. In addition, the PPP is cost effective, mitigates risk, provides constant and rapid supports (protection, detection, response), promotes collaboration and communication, develops a major platform and model for the success of cybersecurity, and increases efforts and defense measures in cyberspace.[44] It has successfully increased

[42] Rachael Thomas, "Securing Cyberspace Through Public-Private Partnership", August 2013, p.15 http://csis.org/files/publication/130819_tech_summary.pdf
[43] Ibid. Rachael Thomas, "Securing Cyberspace Through Public-Private Partnership". pp. 15-16
[44] Intelligence and National Security Alliance "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models". November 2009. p.8

defense against cyber terrorism, hacking, information breaches, and many other cybercrimes. It also coordinated federal, local, and state resources in order to increase communication across government levels and with other international governments and entities.

Furthermore, companies have developed with cybersecurity as a business model. These companies help entities protect information and increase their cybersecurity capabilities. They monitor behaviors, protect the privacy of information, prevent unauthorized users from accessing secure networks, install firewall, antispyware, and encryption software to prevent cybercrimes. Two examples of these companies follow.

The first company is Soltra. Soltra specializes in data protection as well as sharing of information from one private entity to another in order to prevent cybercrimes and develop rapid responses. The company has three major functions[45]:

1) Distilling threat intelligence: this function "de-duplicates data, automates sightings, and prioritizes actions… routes intelligence to users, devices and communities in real time… and reduces the threat indicator analysis lifecycle."[46]
2) Software to receive, process, and route threat intelligence: Soltra uses STIX and TAXII as software to send and process cyber threats to devices, users, firewalls, etc.[47]
3) Automates sharing and trust circle: increases peer to peer sharing as well as sharing with the ISAC in order to combat cyber threats and increase cybersecurity.[48]

---

[45] *Soltra Edge: Robust, Open, Free* Soltra, Accessed November 10th, 2015. http://soltra.com
[46] Ibid. *Soltra Edge: Robust, Open, Free*, Soltra.
[47] Ibid. *Soltra Edge: Robust, Open, Free*, Soltra.
[48] Ibid. *Soltra Edge: Robust, Open, Free*, Soltra.

Soltra began in 2014 primarily based out of the need to protect financial data for banks and other companies in the financial sector. The Depository Trust and Clearing Corporation (DTCC) developed Soltra with the Financial Services Information Sharing Analysis Center (FS-ISAC). The "purpose of this initiative is to develop and distribute a software application and create a network for the automated sharing of security intelligence to protect critical infrastructures."[49] The company now has enhanced information sharing, thus, showing the importance of how that function can be effective on smaller and large scales. The capabilities of companies such as Soltra can significantly increase cybersecurity measures and bolster cyber defenses.

The second company is Tripwire. Tripwire provides and implements cybersecurity services as well. Tripwire partners with Information Technology departments (IT) or develops IT departments for companies in order to secure their cyber networks. For example, Tripwire partnered with Agora, which is a holding company for publishers. Tripwire built new cyber infrastructure for Agora to secure their highly sensitive data and constantly check for any methods of breach into their system. The results were listed in a report. "Solutions: helping the IT team resolve issues…instant alerts to cyber threats and malicious attacks…automated security, compliance, and change control management processes."[50] Agora credited Tripwire with being an instrumental partner in developing cybersecurity infrastructure and resources.[51]

Both of these companies play vital roles in cybersecurity. The examples portray

---

[49] "Cyber Risk-A Global Systemic Threat", A White Paper. DTCC. October 20th,2014. http://www.dtcc.com/news/2014/october/20/cyber-risk.aspx www.dtcc.com/~/media/Files/Downloads/issues/risk/cyber-risk.pdf

[50] *Agora*, Tripwire, 2014.Date Accessed November 15th, 2015. http://www.tripwire.com/register/agora-case-study/

[51] Ibid. *Agora*, Tripwire, 2014.Date Accessed November 15th, 2015.

that partnerships are key to cybersecurity and are necessary to collaborate and develop rapid responses. PPPs are the best method of developing these rapid responses on large scale and international levels.

Issues in Public-Private Partnerships/Cybersecurity

Although PPPs for cybersecurity are an effective means of defending and stopping cybercrimes, there are some issues that come about, thus, creating limitations that can harm the progress of a PPP. This section will discuss the disadvantages of PPPs and the limitations of PPPs in the cybersecurity field. There are generally three disadvantages to PPPs:[52]

1) Legal: PPPs can require a lot of legal framework and documentation. As stated before, when these PPPs cross state and international boundaries many variables come into play that can slow down PPP development.[53]
2) Political Risk: Private sector activities can cause risk for political stability in the public sector. Entities can violate laws and commit other actions that are unethical or illegal.[54]
3) Debt: The public sector can borrow funds upfront, in some cases, and given the long-term timeframe can incur debt if private entities are not meticulous in their activities-poor oversight also can lead to this issue.[55]

Moreover, PPPs also have limitations in the cybersecurity field. PPPs come across limitations in trust, goals, responsibilities, and liability, which can thwart their effectiveness. As a report from New York University states, there are five barriers that

[52] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", pp. 4-5
[53] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", pp. 4-5
[54] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", pp. 4-5
[55] Ibid. Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", pp. 4-5

prevent PPPs in cybersecurity from being effective and developing.[56] These five barriers are:

1) Trust, Control, Risk, and Benefit: There is often mutual distrust between the public and private sectors regarding information sharing. Private entities generally believe in a PPP the government can access their private information, although they do not have access to the government's information. The United States Government (USG) classifies a lot of their information, therefore preventing sharing capabilities. Private companies feel at risk, while the public sector maintains control and purely benefits.
2) Disclosure and exposure: Private sector entities share the sentiment that exposure and disclosure of information to the government puts their entity at risk for litigation and prosecution. It also puts their information at risk for government breaches and leaks.
3) Evolving liability and regulatory landscape: Cybersecurity is a relatively new field, thus laws and regulations are still evolving. Laws and regulations are subject to changes, which could affect PPPs. In addition, private entities could face liability for information shared with the government. Thus, private companies are concerned about liability for unauthorized access of their own information, as well as the risk associated with information accessed by the public sector in the PPP.

[56] Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014. http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

4) Cross-border investigation of cybercrime: Countries vary on the developments and laws in their justice system, thus, it is difficult for PPPs to cross borders as national legal and political conflicts prevent investigations, security, and the detection of cybercrimes. This is the case for many hackers such as Edward Snowden and those of Anonymous, who declared asylum in countries that do not prosecute their crimes.
5) Cross-border data transfer challenges: Data transfer challenges present themselves as entities cross national lines. Countries have different policies surrounding data transfer. For example, in October of 2015, the European Court of Justice "invalidated the US-EU Safe Harbor Framework for data transfer."[57] Data transfer presents problems for the functionality of PPPs.

The three most challenging barriers are the disclosure, exposure, and the cross-border transfer challenges. Private and Public sectors are unwilling to share their information for a variety of reasons. This notion has always caused a rift between the sectors and needs to be faced. The cross-border challenges will continue to grow as cyberspace expands and becomes more integrated. Public and private entities encumbered with diplomatic and cooperation challenges will face imminent issues. Liability will prevent partnerships because entities private or public do not want to be on the hook for a security breach because that entity could then be subjected to criticism and legal action. Barriers in cyber PPPs could potentially prevent their effectiveness.

However, these challenges can be overcome. The creation of an international

[57] *US-EU Safe Harbor Invalidated: what now?,* Proskauer, October 2015. Accessed November 16th, 2015. privacylaw.proskauer.com/2015/10/articles/European-union/us-eu-safe-harbor-invalidated-what-now/

cyber committee with representatives and experts from participating nations could create specific standards of cybersecurity to allow cross-border data transfer and cooperation. In addition, as cyber laws are established parties could create a specific set of laws that apply to international actors. As of now individual countries have applied certain international laws to cyberspace, but more specialized laws with cyber language on an international scale will make PPPs more effective. Lastly, countries could make a set of specific rules for procuring and developing cyber PPPs because of the instantaneous threat that cyberspace presents to world actors and everyday citizens. PPPs can be a crucial tool for cyber defense.

As evidently conveyed, PPPs have disadvantages and limitations in the field of cybersecurity. This does not make developing an effective PPP impossible. Partners must communicate, define goals, declare responsibilities, have great leaders and experts, and cooperate in order to develop a successful PPP for cybersecurity or any industry. PPPs must work through these limitations because the benefits of a PPP definitely outweigh the costs.

Conclusion of this Chapter

In conclusion, PPPs are an effective means of increasing cybersecurity and developing defense in cyberspace. With so many uncertainties in the world, collaboration is the key to effectively stopping threats. The Internet and our digital networks must be resilient in order to fight cybercrimes whether on a small or large scale or a local or international level.

This chapter has discussed the changing nature of security threats in the world today, PPPs, examples of PPPs, and their potential to be a successful tool for the field of

cybersecurity. It is unquestionable that countries and companies recognize the significance of the cyber threats and the role cyberspace is playing in our world. The world is shifting its infrastructure and communications to cyberspace, therefore we must develop PPPs to increase information sharing, build resilient networks, and diffuse cyber threats that can jeopardize the safety of people, services, and operations. As President Obama stated in this year's *National Security Strategy*, "now, at this pivotal moment, we continue to face serious challenges to our national security… escalating challenges to cybersecurity…we will continue to collaborate with established and emerging powers to promote our shared security and defend our common humanity… we will uphold and refresh the international rules and norms that set the parameters for such collaboration."[58]

The world faces potential barriers to PPPs due to the uncertainties related to diplomacy, cooperation, legal framework, and shared liability. Sharing the liability or responsibility of PPPs will make them effective in cyberspace. Cybersecurity must be a global effort with all parties, countries, private entities, and individuals making a concerted effort to form PPPs as an effective method for increasing cybersecurity. Cybersecurity is a necessary public service. The fundamental conclusion is that PPPs must become a common tool in the field of cybersecurity.

[58] "National Security Strategy", White House, February 2015. pp. 15-16
https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

Chapter 2

Introduction and Review of Last Chapter

Today our world exists in a new domain. This domain has instantaneously connected people all over the world. This domain is referred to as cyberspace. Everything exists in this new digital space contained in code and servers. Economic, political, social, and all types of data are now largely dependent upon instantaneous transactions and communications in this new medium. However, the world faces many challenges in the realm of cyber defense. This ability to instantly access all types of data has led to cybercrimes, attacks, and breaches not only of personal data but also of information that is critical to the security of governments and organizations. Recent cyberattacks have included Sony, the Office of Personnel Management (OPM) and other major corporations and governments.

The first chapter explored the use of public-private partnerships (PPPs) in order to combat the growing threat of cybercrimes, cyber-terrorism and warfare. (Public meaning government-run organizations/agencies and private meaning companies that are non-governmental entities). The first chapter argued that PPPs would be an effective tool to bolster cyber defense and increase response time to cyber threats for a variety of reasons including detection, protection, and response mechanisms. The chapter discussed in detail how the PPPs would function, as well as examples of PPPs that exist in the cyber world.

The next step will be to address the crucial question of applying these strategies. Threats are on the rise as the world has become more globalized and dependent upon cyberspace. The question arises: How can these public-private partnerships be applied to defend against cybercrimes, attacks, and breaches? This question is lacking from current

literature on the subject as technology moves faster than literature and law. The literature focuses more on the privacy issues surrounding the sharing of information and not on the effectiveness or ineffectiveness of the PPP model.

The intention of this chapter is to add to the cyber discussion in the area of utilizing the PPP model. This chapter will explore case studies of cybercrimes and apply the public-private partnership methodology to these case studies to establish if a general set of PPP guidelines and functions can facilitate better response time for cyber threats and increase cybersecurity as a whole. This chapter will discuss case studies including Sony, Target, financial entities like Citigroup and JP Morgan Chase, and OPM. The chapter will also discuss the Apple case and privacy issues that have arisen from these partnerships. The application of the PPP model can be crucial in order to increase cybersecurity and prevent future crimes.

Literature Review

Cybercrimes are occurring at a rapidly increasing rate. The cyber world has forever changed the face of worldwide interaction and communications. Terrorism, theft, information breaches, and many other crimes have become possible based upon the far reaching capabilities of the cyber world. It is the first medium that changes instantaneously as well as leaves people vulnerable to the constant threat of crimes. In addition, so much of the world's daily communications depend on access to the cyber world. These communications have altered the means in which political, economic, and social interactions occur on a daily basis. In 2011, Richard W. Downing, who at the time was the Deputy Chief of Computer Crime and Intellectual Property Section of the Department of Justice (DOJ) Criminal Division, testified at a Judiciary Committee

Hearing for the House of Representatives. He stated "that the United States confronts serious and complex cybersecurity threats. The critical infrastructure of our Nation is vulnerable to cyber intrusions that could damage vital national resources and put lives at risk, and intruders have also stolen vast databases of financial information and valuable intellectual property."[59] In other words, cybersecurity presents a troubling issue for the U.S. and the world.

The use of public-private partnerships has slowly been implemented into the cyber world. These partnerships allow the rapid exchange of information between the public and private sectors in order to slow down the effects of cybercrimes. But these partnerships have caused a lot of controversy. Private companies do not want to share their information with the government. On the flip side, the United States Government (USG) tends to over classify threats and other information as national security which leads to the private sector not feeling secure about the USG's knowledge, capabilities, or intentions. Thus, two schools of thought have developed. One side of the spectrum rests with those who hold that private companies and the public sector should share information on cyber threats and crimes in order to combat these issues. The other side of the spectrum rests with those who believe that the private sector should keep their information and operations separate from the public sector agencies. This literature review will look deeper into these privacy issues as they play a major role into applying the public-private partnership model.

The balance of sharing information and protecting privacy presents itself within a gray zone. This issue has been going on for some time. At the same Judiciary Committee

[59] House. Judiciary Committee. *Cyber Security: Protecting America's New Frontier,* 112th Cong., 1st sess. H. Rept. 112–80. November 15th 2011. Accessed February 25th 2016. Page 5.

Hearing in 2012, Congressman Bobby Scott presented the issue of sharing information. He stated that, "[I]t is critical that we work together in Congress with the Administration and with the business community and with private advocates to find ways to enhance the security of our government information systems, our business computer networks and the personal use of the Internet…but I note concern about proposals to expand the ability of private companies to share information with government and ultimately with law enforcement for the purpose of protecting against cyber security threats. If we allow vastly overbroad sharing of information, we actually may undermine the very privacy rights which should be at the forefront of our concern."[60] The issue of sharing information to facilitate security is on the rise.

Those who oppose the sharing of information between the private sector and the public sector rely on arguments of privacy rights and a lack of security on government servers. Two cases highlight this scenario. The first is the recent Apple case. The Federal Bureau of Investigation (FBI) subpoenaed Apple to force the company to break the encryption of a phone allegedly related to terrorist activities. But Apple along with a number of other major private corporations held its ground and would not submit to the FBI's demand to break the encryption. Apple's General Counsel, Bruce Sewell, testified in Congress. Sewell, in his testimony argued that "creating such software would undermine anti-hacking security for all iPhones."[61] Another witness in his prepared testimony stated that "the line between personal privacy and public safety should be

[60] Ibid. House. Judiciary Committee. *Cyber Security: Protecting America's New Frontier*. pp.3-4
[61] Anlina Selyukh, "FBI Chief and Apple's Top Lawyer head into First Encryption Hearing". NPR. March 1, 2016. Accessed April 4th, 2016.
http://www.npr.org/sections/thetwo-way/2016/03/01/468599364/fbi-chief-and-apples-top-lawyer-head-into-first-encryption-hearing

drawn by Congress."[62] In other words, people on this side of the coin feel that partnerships are a negative tool as sharing of information between the private and public sectors should be limited or nonexistent, but if laws were to change those changes should be left to Congress and not to government agencies. The development of partnerships has been much more successful with financial companies. Some technology companies have resisted these partnerships. Google, Microsoft, and many other companies are filing briefs in support of Apple.[63] This paradox is interesting. Opening the door for the government to compel private corporations to share information can lead to the end of privacy in the eyes of many.

Furthermore, the OPM hack has played into this issue of security and privacy as well. Many are concerned that the government's cybersecurity is not as secure as private companies. Besides the millions of people with sensitive information now accessed by unauthorized users (alleged Chinese hackers), many feel the government had some major cybersecurity failures. According to Wired, "the agency (OPM) was harshly criticized for its lax security in an inspector general's report released last November [2014] that cited its lack of encryption and the agency's failure to track its equipment. Investigators found that the OPM failed to maintain an inventory list of all of its servers and databases and didn't even know all the systems that were connected to its networks. The agency also failed to use multi-factor authentication for workers accessing the systems remotely from home or on the road."[64] This hack raised the question of the strength in public sector

[62] Ibid. Anlina Selyukh, "FBI Chief and Apple's Top Lawyer head into First Encryption Hearing". NPR. March 1, 2016. Accessed April 4th, 2016.
[63] Anlina Selyukh, "FBI Chief and Apple's Top Lawyer head into First Encryption Hearing". NPR. March 1, 2016. Accessed April 4th, 2016.
[64] Greenberg and Zetter, "Why the OPM Breach is such a Security and Privacy Debacle". Wired June 11th, 2015. Accessed March 3rd, 2015. http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/

security which is alarming for many people. Some in the private sector do not trust the public sector security and will not enter into partnerships that could potentially make them vulnerable.

Both of these issues were highlighted in Judith's Germano's (Professor at the NYU School of Law and Fellow at the Center on Law and Security) piece entitled "Cybersecurity Partnerships: A New Era of Public-Private Collaboration". She described that trust and control and disclosure and exposure are some of the concerns of private entities when dealing with public sector partners.[65] She wrote, "there also is a significant concern that information sharing often is a one-way relationship: the government accepts information that companies share, but is not always capable of rendering tangible assistance in return... Yet another barrier to effective public-private sector cooperation is the matter of disclosure and exposure. Many companies remain reluctant to reveal security vulnerabilities, especially before they fully have assessed the scope of the problem. They are concerned that doing so will mean they could face negative press, regulatory scrutiny, and civil litigation."[66] The Apple case brought to light that government access and interference may not be the best path for cybersecurity as private entities feel subject to regulation and scrutiny from public agencies. In addition, the OPM hack showed that government systems may not be as secure as some private systems. These issues of privacy can plague the ability of these partnerships to function effectively.

---

[65] Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014. p.3
http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

[66] Ibid. Judith Germano "Cybersecurity Partnerships: A new Era of Public-Private Cooperation". October 2014. p.3

On the other hand, many still believe in the strength of these partnerships to increase cybersecurity. The Sony hack highlights the strength of these partnerships. Sony Chief Executive Officer (CEO), Michael Lynton, and Aspen Institute CEO Walter Isaccson recounted the hack in a DOJ press release.

> Carlin and Lynton recounted the story of the hack and highlighted Sony's valuable cooperation with law enforcement. They emphasized the role that public-private partnerships play in averting cyber hacks and mitigating their damage. Carlin said that Sony's willingness to involve law enforcement immediately was 'an important lesson that Sony did right.' 'Literally within hours of the original breach – within the first 24 hours – Sony reached out and the FBI had a team go to Sony to assist'…to this end, Carlin announced an NSD (National Security Division, DOJ) outreach initiative to promote information sharing and resilience, as well as to help private companies protect themselves and respond to cyber intrusions.[67]

The Sony case portrays the concept that the public and private sector can work together to facilitate successful partnerships that can counteract cybercrimes while upholding privacy and other rights. These themes will continue to remain prevalent in our world today.

This idea of trust in the government may stem from an issue related to the way in which people view their privacy. Matthew Easton, a professor at the University of Austin, describes that there should be a change in the way that people view their privacy in cyberspace.

> [T]he nature of digital communication suggests a need to rethink this definition for the modern age. An individual's digital identity encompasses a wide range of traceable offline characteristics (e.g., age, residence, income, etc.) in addition to a variety of online profiles, passwords, pin numbers, access codes, and behaviors all of which establish concrete links between social and technological understandings of identity. Today's digital consumer is no longer entirely anonymous since virtually every form of

---

[67] *Readout of Assistant Attorney General for National Security John P. Carlin's Address at Vanity Fair's 2015 New Establishment Summit,* Department of Justice, Press Release, Tuesday, October 6, 2015. Accessed March 3rd, 2016. https://www.justice.gov/opa/pr/readout-assistant-attorney-general-national-security-john-p-carlin-s-address-vanity-fair-s

> communication and behavior generates data that can be collected, aggregated and analyzed.[68]

The point being that individuals and private companies may have to revisit their fundamental values and recognize that without the help of the public sector, their cybersecurity is susceptible to existential threats. Private sector entities may have to give in on some of their privacy concerns to better cybersecurity as a whole.

Furthermore, this issue of sharing information was also discussed in a paper by the Center for Democracy and Technology. The argument was that no one organization can be safe as cyberspace is too complex and vast for one entity to protect themselves. "Given the complexity and interconnected nature of information systems and networks, as well as an ever-evolving and sophisticated threat environment, no one organization or entity can address United States (US) national cybersecurity alone. Industry players must work together, government entities must harmonize their approaches to protecting critical infrastructure, and government and industry must work together to address common concerns and build collaborative solutions."[69] In other words, forfeiting some privacy concerns may be necessary in order to develop successful partnerships as security should trump the other issues at play.

The debate has been a pivotal topic of discussion since the issue of privacy has been put to the test in connection with cyberspace issues. The public has differing viewpoints on the issue. A Pew Research Center study showed that the public is subjected to event influences. For example, after the Snowden leaks, 47% of people in a

---

[68] Matthew Easton, *Living in a Big Data World*. ScienceDirect. Vol 58. January 14th, 2016. Accessed March 3rd, 2016. http://www.sciencedirect.com/science/article/pii/S0747563215303216

[69] "Improving our Nation's Cybersecurity through the public-private partnership", Center for Democracy and Technology, March 8th, 2011. p.4 https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf

study criticized the anti-terror surveillance programs; however after San Bernardino in December of 2015, 56% of the survey called for more government surveillance.[70] Moreover, this appears to be the flaw in literature. There is more written about privacy concerns and the balance of civil liberties than how these partnerships could be enhanced in order to bolster cybersecurity. The privacy issue is important, however, it should not take away from the discussion on PPPs and their effectiveness in the cyberspace world. Therefore, the following case studies will discuss the effectiveness of these partnerships, as a necessary element of cyber defense, despite privacy concerns.

Case Studies

The intention of this argument is to introduce the idea that PPPs could be effectively applied to cybersecurity defense policy as a method of drastically increasing response-time to real threats. As previously discussed, a cyber threat will be defined as a "circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society."[71] Cybercrimes will be defined as criminal offenses committed via the Internet or otherwise aided by various forms of computer technology.[72] These actions include terrorism, hacking, theft, unauthorized access, information dissemination, fraud, scams, copyright of code, and many other crimes that exist on computer, smartphone, or any digital networks. Readers

[70] Shiva Maniam and Lee Rainie. *Americans feel the tension between privacy and security concerns.* Pew Research Center. February 19th, 2016. Accessed March 4th, 2016. http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

[71] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, Feburary10th, 2015, Accessed November 10th, 2015. https://definedterm.com/a/download/document/11128

[72] *Cybercrimes,* FindLaw, Accessed November 10th, 2015 http://criminal.findlaw.com/criminal-charges/cyber-crimes.html

may refer to the appendix for a glossary of other terms. The PPP model can be utilized to reduce the risk of cyber threats and decrease the presence of cybercrimes. The PPP model would include the three major goals of detection, protection, and response. The following section will discuss some past cyber-related events and apply the PPP model to those case studies.

Sony

In December of 2014 a group of hackers, known as the Guardians of Peace hacked Sony Pictures Entertainment under the alleged sponsorship of North Korea. The reason for the hack was in response to Sony's film *The Interview,* which featured a plot of Kim Jong-Un, the North Korean Leader, being assassinated.[73] The hackers committed a cybercrime of theft of information. The hackers stole and leaked personal information, embarrassing emails, and other private information from Sony. Besides costing the studio millions, the cyber theft of this information instilled fear in movie theaters, most of whom pulled the movie from theaters.[74] The act was more than a simple cybercrime. It was a diplomatic act of aggression on the international stage. The act brought such weight, that President Obama felt compelled to criticize the CEO of Sony for pulling the picture from theaters. President Obama, in a press conference, said "We cannot have a society in which some dictators someplace can start imposing censorship here in the United States because if somebody is able to intimidate us out of releasing a satirical movie, imagine what they start doing once they see a documentary that they don't like or news reports

[73] *The Interview Plot Summary*. IMDB. Accessed March 3rd, 2016. http://www.imdb.com/title/tt2788710/plotsummary

[74] Frederick Brown. *The Sony Hack: One Year Later*. CNBC. Nov, 24th 2015. Accessed March 8th 2016. http://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html

that they don't like…[T]hat's not who we are. That's not what America is about."[75] Obama recognized the need for better diplomatic response as a private corporation of the United States became vulnerable on an international stage.

The FBI investigation linked malware and hacking techniques to a certain group of hackers.[76] Malware is software that compromises the operation of a system by performing an unauthorized function or process.[77] This is vital as it plays into the discussion of a PPP for cybersecurity. As Senator Diane Feinstein stated in 2014, "the onus is on the government and the international community to act in the face of this cyberattack."[78] There must be a consensus or partnership between the private and public sector as in cyberspace private companies with major global influence are vulnerable to cyber threats on a constant basis.

The partnership would function as a tool for real-time response to cyberattacks. As Madeline Carr, a professor at Cardiff University, wrote "*partnerships as power sharing* are based on an ethos of cooperation where 'trust replaces the adversarial relations endemic to command-and-control regulation' and where there is some mutually beneficial sharing of responsibility, knowledge or risk."[79] The partnership is interdependent on both parties or multiple parties performing their duties with the expectation that the other party will follow their end of the deal. As laid out in the first

---

[75] Evan Perez, *Obama 'Sony Made a Mistake*. CNN Politics. Dec, 19th 2014. Accessed March 8th, 2016. http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/

[76] Ibid. Evan Perez, *Obama 'Sony Made a Mistake*. CNN Politics.

[77] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, Feburary10th, 2015, Accessed November 10th, 2015. https://definedterm.com/a/download/document/11128

[78] Ibid. Evan Perez, *Obama 'Sony Made a Mistake*. CNN Politics.

[79] Madeline Carr. *Public-Private Partnerships in national cyber-security strategies*. International Affairs, 2016. p. 57
https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

chapter, the PPP would function as follows. There would be a control or executive board. This board would consist of members from both parties. In this case, there would be members from Sony as well as the DHS, FBI, National Security Agency (NSA), or any government agency in on the partnership. The executive board would establish the goals of the partnership. In this case, the goals would be increasing the cybersecurity and cyber defense of Sony as their actions affect the global realm of cyberspace. As Carr also wrote, "it becomes clear that despite this complexity and diversity, the core focus in the strategies (and consequently in this article) is on the relationship between the government and the owners/operators of critical infrastructure—the rationale being that, while the many other aspects of cybersecurity are regarded as linked to the national *interest*, critical infrastructure protection is unequivocally and intrinsically linked to national *security*."[80]

In addition, the funding for the partnership would be handled through the private sector party, which would pay for any hardware or monitoring that is necessary to enhance security. This allows the partnership to function without the so-called bipartisan "red tape" of the government. The instant that Sony's software detected the malware, that signal would be instantaneously transmitted to the monitoring government agency, who would run the check on the malware and the systems of the partnership to identify the source. The delayed response with Sony unaware of the hack until the information had already been leaked potentially could have been reduced. The response time could have been instantaneous protecting the privacy of individuals as well as the private corporation. Furthermore, the public agency could then probe its other partnerships and

[80]Ibid. Madeline Carr. *Public-Private Partnerships in national cyber-security strategies.* International Affairs, Chatham House. 2016. P. 45.

major systems for the same piece of malware as well as alert other parties of the threat. This would enable other systems to increase their cyber defenses.

In essence, the PPP would serve several major purposes, also portrayed in figure 1.3 (Appendix 1), by the manner in which it functions.[81] The PPP would regulate, inspect, and enforce compliance from suppliers and users. Examples of suppliers are telecommunications companies, software suppliers and Internet Service Providers (ISPs) and users can be any party or entity on the Internet. In addition, the partnership would provide detection from cyber threats and contribute to response and recovery through information sharing. Furthermore, while performing these functions the PPP will strive to protect the individual privacies and liberties of users and suppliers. This is a crucial function in order to promote collaboration and information sharing on both national and international levels.

Sony did ask for help from the USG after it had been hacked. Sony would benefit from consistent participation in a PPP as detection, protection, and response mechanisms would maintain Sony's security and prevent cyber-attacks from occurring in the first place.

Target

In November of 2013 Target, a major retail store, experienced a severe hack of their data systems. Target announced on December 19th, 2013 that over 40 million credit and debit cards had been stolen.[82] This originally just included the name on the card, card

---

[81] "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models", Intelligence and National Security Alliance, November 2009. p.9 http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

[82] McGrath, Maggie. *Target Data Breach Spilled Info On as Many as 70 Million Customers*. Business Insider. Jan. 10th, 2014. Accessed March 10th, 2016. http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#27095bea6bd1

number, expiration date, and the card verification value. However, a month later in January of 2014, Target announced a change in their report after investigation into the hack. Target recognized that an additional 70 million people could have been affected with information including their names, addresses, phone numbers, and other personal information.[83]

The hackers targeted point-of-sale systems, or the machines and computers that read and store the credit card information of customers when they make purchases. This version of cyber theft is more recent. Hackers target the vulnerability of major businesses and companies. The New York Times described how the hack functioned. "To pull it off, security experts said a company insider could have inserted malware into a company machine, or persuaded an unsuspecting employee to click on a malicious link that downloaded malware that gives cybercriminals a foothold into a company's point-of-sale systems."[84] Over a month span cybercriminals copied this private information of customers and gained the ability to produce fake cards, purchase items, steal identities, and commit a number of cybercrimes. Fear broke out as people realized that their sensitive information had been stolen and was in the hands of unknown cybercriminals.

The existence of a PPP potentially could have saved Target from spending $61 million initially in response to the breach, and billions on lawsuits, remediation, and other costs connected to the data breach of their systems.[85] As the paper from the Center for

---

[83] Ibid. Maggie McGrath. *Target Data Breach Spilled Info On as Many as 70 Million Customers*. Business Insider

[84] Nicole Perlroth *Target Investigates Breach Involving Credit Card Data*. New York Times. Dec. 18th, 2013. Accessed April 10th, 2016. http://bits.blogs.nytimes.com/2013/12/18/target-looking-into-security-breach/?hpw&rref=technology&_r=0

[85] Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014. p.4 http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

Democracy and Technology stated:

> [t]he success of the [public-private] partnership depends on articulating the mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often more difficult to articulate the direct benefits of participation for the private sector....In assessing the value proposition for the private sector, there is a clear national security and homeland security interest in ensuring the collective protection of the Nation's [critical infrastructure and key resources].[86]

A partnership for Target could have saved it from mass security failure and profit loss, while protecting the information security for citizens that use Target. The partnership would serve major functions such as providing accurate and timely information to owners and operators, engaging Target in cybersecurity initiatives, setting policies and goals that protect Target and bolster national security, creating an environment for Target and other companies to engage in these partnerships through support and incentives, and lastly providing research and support for future security systems and concerns.

In addition, the information sharing of the partnership would focus around "an analysis of the respective roles of the private sector and the government and by a better understanding of the collective or collaborative action needed to combat current or future attacks."[87] This would have two purposes. First, the information sharing would identify requirements and responsibilities and build the capacity of those sharing mechanisms. For example, in the Target case study, Target would have shared its malware identification with a monitoring government agency, which would then have run checks through Target and other systems. This does not diffuse the responsibilities, but instead it enhances the

[86] "Improving our Nation's Cybersecurity through the public-private partnership", Center for Democracy and Technology, March 8th, 2011. p.6 https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf
[87] Ibid. "Improving our Nation's Cybersecurity through the public-private partnership", Center for Democracy and Technology, March 8th, 2011. p.14

roles and overall security of private and public information systems. With these partnerships and supports in place, Target could have recognized the attack promptly, thus more likely preventing the theft of data over two months from Target's digital systems.

Furthermore, the second purpose of this information sharing partnership would enable Target to only share data that appears to threaten the system. This would not include routine data sharing. "Information sharing also needs to evolve with modern threat patterns… (which) shifts the focus from sharing inbound attacks and technical vulnerabilities to unauthorized outbound traffic and needs to be developed. Since many modern attacks such as advanced persistent threats (APT) are not successful until data is exported from the system, managing unauthorized URLs and websites can be an effective defense."[88] Therefore, Target could protect the civil liberties of its customers and adhere to privacy concerns, while having an effective cybersecurity strategy and system that can combat modern cyber threats and cybercrimes. The development of a PPP with Target and a government agency could enhance security for Target, its customers, and other public and private entities that share similar vulnerabilities.

Citigroup and JP Morgan Chase

The hacks of Citigroup and JP Morgan Chase, two worldwide financial institutions, are other case studies for applying the PPP model. In June of 2011, Citigroup was hacked when an unknown group stole millions from customer's accounts.[89] In October of 2014, "JP Morgan, revealed in an SEC filing that more than 70 million

[88] "Improving our Nation's Cybersecurity through the public-private partnership", Center for Democracy and Technology, March 8th, 2011. p.15

[89] Aaron Smith. *Citi: Millions Stolen in May Hack Attack*. CNN Money. June 27th 2011. Accessed April 16th 2016. http://money.cnn.com/2011/06/27/technology/citi_credit_card/

households and seven million small businesses may have had their private data compromised in a cyberattack."[90] Both hacks are interesting as both companies are large financial institutions with global influence.

These case studies are interesting because the big world banks of Wall Street recognized the need for data sharing. Thus, Soltra was born. Soltra began in 2014 primarily based out of the need to protect financial data for banks and other companies in the financial sector. The Depository Trust and Clearing Corporation (DTCC) developed Soltra with the Financial Services Information Sharing Analysis Center (FS-ISAC). The "purpose of this initiative is to develop and distribute a software application and create a network for the automated sharing of security intelligence to protect critical infrastructures."[91] The company now has enhanced information sharing, thus, showing the importance of how this function can be effective on smaller and large scales. Soltra is working to conquer the issues of trust and control and disclosure and exposure that have plagued the development of many information sharing vehicles. Soltra balances both public and private interests while increasing cybersecurity. Soltra provides a method for firms such as Citigroup, JP Morgan Chase, and many other large world banks and financial institutions to share cyber threat information electronically. As the paper from the Center of Democracy and Technology provided, "Sector-designated information-sharing mechanisms, such as the ISACs, are now integrated into the public-private partnership framework. Some sectors, such as finance, information technology and

---

[90] Portia Crowe. *JP Morgan fell victim to the largest theft of customer data from a financial institution in U.S. History*. Business Insider. November 10th 2015. Accessed April 17th 2014. http://www.businessinsider.com/jpmorgan-hacked-bank-breach-2015-11

[91] "Cyber Risk-A Global Systemic Threat", A White Paper. DTCC. October 20th,2014. http://www.dtcc.com/news/2014/october/20/cyber-risk.aspx www.dtcc.com/~/media/Files/Downloads/issues/risk/cyber-risk.pdf

communications, are well known to have strong and proven information-sharing capabilities."[92] The capabilities of information sharing companies can significantly increase cybersecurity measures and bolster cyber defenses. The success of financial PPPs is an important example to prove that these partnerships can be applied in the world today despite issues that may arise.

Office of Personnel Management (OPM)

The hack of the OPM, which was mentioned in the earlier sections of this paper, is also an important point of discussion. OPM is not a private entity. It is a public agency of the USG. In July of 2015, OPM was hacked by a group allegedly from China. The data breach exposed millions of government employees' personnel information and showed the vulnerability of certain government cyber systems to the world. This case study is important because it exemplifies the capabilities of information sharing as a powerful tool to be proactive against cyberattacks. This concept was discussed by Scott Shackelford, a senior fellow at the Center for Applied Cybersecurity Research. "Instead, the proactive cybersecurity movement includes technological best practices ranging from real-time analytics to cybersecurity audits promoting built-in resilience, and may be considered to be a response to the more reactive stance of an array of companies…such an approach represents an opportunity for firms to create broad, collective defense partnerships".[93] In other words, partnerships are instrumental for bolstering cyber defenses of private and

[92] "Improving our Nation's Cybersecurity through the public-private partnership", Center for Democracy and Technology, March 8th, 2011. p.14 https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf
[93] Shackelford, Scott. *Protecting Intellectual Property And Privacy In The Digital Age: The Use Of National Cybersecurity Strategies To Mitigate Cyber Risk*. Chapman Law Review. 2016. Page 16. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2635035

public entities.

This concept is crucial as the hack of OPM portrayed to the world that cybercrimes are asymmetric. William Lynn defined asymmetric, when discussing the Pentagon's cyber strategy, as "the low cost of computing devices means that U.S. adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to US military capabilities. A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the US global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target."[94] Although Lynn is focusing his discussion on more of a military and defense based concept, it is still important to recognize that both private and public entities become targets in cybercrimes and there is always an imminent threat to companies and public agencies that play important roles in the global system.

Cyberspace makes all parties vulnerable, thus, Shackelford proposes the concept of the National Institute of Standards and Technology (NIST) Framework for partnership building. "The Cybersecurity Framework harmonizes consensus standards and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk."[95] In essence, the NIST framework is a great example of partnership building in order to enhance cybersecurity and relationships among all entities and agencies.

---

[94] William Lynn. *Defending a New Domain*. Foreign Affairs, Vol. 89 No. 5 (October 2010). pp 98
[95] Shackelford, Scott. *Protecting Intellectual Property And Privacy In The Digital Age: The Use Of National Cybersecurity Strategies To Mitigate Cyber Risk*. Chapman Law Review. 2016 p. 17. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2635035

Lastly, the Department of Defense (DOD) conducted a review of some of their PPPs in order to assess their functionality and effectiveness. The Task Group found that DOD PPPs were divided into cyber defense, research, humanitarian aid, family support programs, and a few other categories. The Task Force established that the PPPs had common elements: "it is an interaction between a DOD component and a private entity; it is voluntary, not mandated or part of an organizational framework; the bywords are 'mutual' and 'shared' this would include mutually agreed goals and governance, and shared decision-making; private sector includes not only corporations, but also Non-Governmental Organization (NGOs), universities, foundations, community-based and other private sector organizations; almost any kind of entity other than the UN or another country; and other federal agencies may also be involved, although normally in conjunction with a private sector entity." [96] These elements make PPPs more effective in securing cyberspace as the private and public sectors cannot remain alone to fight these cyber challenges. The Task Group reported that, "PPPs are the next step in the evolving 'whole of government' and 'whole of society' collaboration models – a resource needed now more than ever as the Department faces new challenges and threats in an era of declining resources."[97] The development of PPPs can change the face of cyberspace defense and information sharing as well as bolster cybersecurity.

Limitations

Despite the application of PPPs in these case studies there are some limitations.

---

[96] *Report to Secretary of the Defense: Public Private Collaboration in the Department of Defense. 2012* Defense Business Board. p.2
http://dbb.defense.gov/Portals/35/Documents/Reports/2012/FY12-4_Public_Private_Collaboration_in_the_Department_of_Defense_2012-7.pdf

[97] Ibid. *Report to Secretary of the Defense: Public Private Collaboration in the Department of Defense. 2012*. Defense Business Board. p.27

Germano in her paper describes some of these limitations. She wrote, "major categories of obstacles to effective cooperation between public and private actors combatting pervasive cyber threats include: (1) issues surrounding trust and control of incident response; (2) questions about obligations regarding disclosure and exposure; (3) the evolving liability and regulatory landscape; (4) challenges faced in the cross-border investigation of cybercrime; and (5) cross-border data transfer restrictions that impede the ability of companies to respond nimbly to cyber threats and incidents."[98] The issues of trust and control as referenced in the OPM case study, or the fact that government systems could not be secure, present an issue for establishing these PPPs. In addition, companies like Apple and other technology giants have resisted these partnerships for issues of disclosure and exposure. Companies are concerned their privacy will be violated and interfered with by government programs and policies. This is a major concern as privacy issues are prevalent in the establishment of PPPs. Furthermore, the evolving landscape of cyberspace presents a challenge for partnerships as the legal aspects of cyberspace are still be ironed out. For example, the privacy case with Apple and other technology companies will threaten the success of these partnerships. The final issue at hand is the cross-border enforcement and data issues. The US is one of the leaders in cyberspace. However, not all countries have the same capabilities and data guidelines, thus, presenting many cybersecurity challenges for PPPs. The lack of coherent laws and capabilities in cyberspace will continue to plague the development of PPPs until these issues are worked out on a global scale.

[98] Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014. p.3
http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

Conclusion of this Chapter

Although there are many challenges and limitations in cyberspace, PPPs can be an effective tool for increasing cybersecurity. The exploration of these case studies portrays that PPPs can be applied in an effective manner to thwart cybercrimes. PPPs present a means through which successful partnerships can be developed in order to balance both public and private sector interests, while increasing cybersecurity as a whole. The case studies of Sony, Target, Citigroup, JP Morgan Chase, and OPM all are examples in support of the cyber PPP as a mechanism for bolstering cyber defense. As a society, it would be best to place the privacy issues in perspective and develop these partnerships for the security of our critical cyber infrastructure, which is now necessary for most daily activities on a local, state, federal, and international level.

The next chapter will discuss the laws surrounding cyberspace and delve more into the privacy issues. The instantaneous nature of cyberspace is too fast for national and international legal systems as they exist today, thus, the focus will be on the laws and policies that exist and recommendations to alter some of these in order to secure cyberspace in the future.

Chapter 3

Introduction and Review of Previous Chapters

The development of cyber technologies has altered the way in which interactions occur on a daily basis at the individual, local, national, and international levels. Communications, data transfer and storage, commerce, business, and military affairs are now dependent on the Internet and other cyber technologies. In essence most of the world's social, political, and economic interactions occur through this new domain, which is commonly referred to as cyberspace. The National Initiative for Cyber Security Careers and Studies (NICCS), developed by the Department of Homeland Security (DHS), defines cyberspace as "the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[99]

There are numerous benefits to cyber technology and the accessibility of cyberspace. Individuals, private businesses, and governments can access information and perform a myriad of functions through a device connected to cyberspace. In addition, the large scale development and use of cyberspace has allowed a new level of interconnectedness. People are instantaneously connected on a global scale with the ability to disperse news, knowledge, and any type of information through this connective ability.

However, a broad array of security issues has arisen due to the vulnerabilities of cyberspace. One person accessing the Internet can commit a wide range of cybercrimes

[99] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, Feburary10th, 2015, Accessed November 10th, 2015. https://definedterm.com/a/download/document/11128

that threaten the safety and security of individual people, the private sector, and the public sector. A cybercrime is defined as criminal offenses committed via the Internet or otherwise aided by various forms of computer technology.[100] These actions include terrorism, hacking, theft, unauthorized accessing of information, information dissemination, fraud, scams, copyright of code, invasions of privacy and many other crimes that exist on computers, smartphones, and/or any digital networks. (A full list of definitions of cybercrimes and other technical related terms can be accessed through the NICCS link in the glossary).[101] The accessibility of systems and cyber-related technologies makes threats and cybercrimes imminent. Both civilian and military systems are vulnerable to these threats and crimes. The applications of these cybercrimes are extensive. Entire power grids, civilian heath care communications, military communications, satellites, weapons, and access to, and privacy of, personal data can all be jeopardized by cybercrimes.

Furthermore, cyberspace is a domain in which technology and capabilities make a country or entity more vulnerable. In other words, there is an asymmetric element when it comes to cyber technologies. The more a private or public entity becomes intertwined and dependent in cyberspace, the more vulnerable that entity becomes to cybercrimes. Myriam Dunn Cavelty who is the head of the New Risks Research Unit at the Center for Security Studies at ETH Zurich, Switzerland and coordinator of the Crisis and Risk Network, describes the issue of asymmetry in cyberspace in her paper, "Critical

---

[100] *Cybercrimes,* FindLaw, Accessed November 10th, 2015 http://criminal.findlaw.com/criminal-charges/cyber-crimes.html

[101] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, Feburary10th, 2015, Accessed November 10th, 2015. https://definedterm.com/a/download/document/11128

Information Infrastructure". She wrote:

> Fear of asymmetric measures against such targets has been aggravated by the so-called information revolution. Today, almost all Critical Infrastructure (CI) relies on a spectrum of software-based control systems for smooth, reliable and continuous operation. In many cases, information and communication technologies (ICTs) have become omnipresent, connecting infrastructure systems and making them interrelated and interdependent. The part of the information infrastructure that is essential for the continuity of CI services is known as critical information infrastructure (CII). CII is thus part of a state's CI and includes components such as computers, software, the Internet, satellites and fiber optics…Attacking infrastructure therefore has a "force-multiplier" effect that allows even a relatively small attack to achieve a great impact. The spread of ICT appears to make the post-Cold War asymmetric threat easier; facilitating access to the tools for attack, and making the success of an attack more likely. Borders, which are already porous in the real world, are non-existent in cyberspace.[102]

In other words, entities without strong economic, political, or military power and organization can achieve their goals through committing cybercrimes on cyber systems.

The vulnerabilities and asymmetrical nature of cyberspace has brought to light a major issue of cybersecurity. This is the lack of cooperation between the public and private sectors. The private sector has more resources available in its arsenal, however lacks the will to work with the government out of fear of regulation and privacy invasion. The public sector desires to control the parameters but lacks the technical skill and resources to perform a functioning cybersecurity model on its own accord. Therefore, the need for public-private partnerships (PPPs) has developed out of a growing concern of cybercrimes and the need for better cybersecurity on a multilateral level. Cavelty discusses the need for cooperation in her paper as well. She points out that the provision of critical services has been privatized. Therefore, critical information and technical

[102] Myriam Dunn Cavelty, "Critical information infrastructure: vulnerabilities, threats and responses". *Disarmament Forum.* 2007. p.16

resources largely sit within the private sector. However, due to a multitude of financial priorities private sector entities do not always allocate resources to maximize cybersecurity. On the other hand, the government sets the protection standards that it expects the private sector to follow.[103] "In order to gain the support of the private sector without having to introduce heavy regulation, governments must strive to create a mutual win–win situation."[104]

Moreover, this is where the need for PPPs takes hold of the current situation in cybersecurity. Digital systems are vulnerable and the need for strong security in this domain is vital as it is critical to everyday life for military and civilian operations. However, currently there are a lack of partnerships. The lack of PPPs is due to many reasons. First, there is a lack of literature on the subject, making theory and studies behind cyber issues difficult to ascertain. There is a gap between theory, education, development, and logistical application. This is an ongoing issue for cyberspace as logistics and development have not caught up to reality and necessities for cybersecurity. Second, the field is relatively new to the world and evolves on a constant basis. An individual can have a monumental effect on cyberspace with access to the Internet from a single device. Third, PPPs are difficult and complicated. They involve the public and private sectors, a variety of operational factors, and require a heavy amount of work to develop and sustain a lasting partnership. Fourth, a large amount of electronic information is classified and inaccessible due to the imminent and instantaneous nature of cyberspace, therefore, making policy and law difficult to develop. Lastly, cyberspace also

[103] Ibid. Myriam Dunn Cavelty, "Critical information infrastructure: vulnerabilities, threats and responses". p.19
[104] Ibid. Myriam Dunn Cavelty, "Critical information infrastructure: vulnerabilities, threats and responses". p.19

requires international cooperation from legal documents through logistical application and sharing of information. These issues build upon each other as cyberspace becomes more complicated and intertwined with daily operations of individuals, public entities, and private entities.

In addition, recent cyberattacks and crimes against major public and private entities have highlighted some of these growing concerns on the global stage. Hacks on Sony, Target, Citigroup, JP Morgan Chase, the Office of Personnel Management (OPM) and other public and private entities have raised security concerns for personnel, economic, social, and political data. It appears that very few cybersecurity systems are secure on their own. The case studies of recent cyberattacks provide the evidence for this claim. The previous chapters addressed some of the questions surrounding these issues with cybersecurity and the lack of presence of PPPs.

The first chapter of this thesis asked the question: What is necessary to increase cooperation in order to enhance cybersecurity? The answer to this question was for the development of cyber public-private partnerships as an effective means to combat growing security issues. The components of the chapter described the elements, technicalities, effectiveness, purposes, and advantages of PPPs. The argument then focused on the effectiveness of PPPs for cybersecurity. This is done by increasing cooperation and collaboration between the public and private sectors as well as increasing detection, and protection, and decreasing response time to cyber threats and cybercrimes. The enhanced capabilities of information sharing would allow vast monitoring of cyber systems for real security threats by unauthorized users. Lastly, the chapter discussed some examples of current cyber PPPs as well as limitations on their development. The

PPP model portrays evidence that cyber partnerships can function effectively and enhance cybersecurity systems.

The second chapter of this thesis asked the question: How can these partnerships be applied in order to bolster cybersecurity? The main argument of the chapter applied the PPP model to recent cyber case studies in order to demonstrate their effective characteristics. The case studies included in the chapter included Sony, Target, Citigroup, JP Morgan Chase, and OPM. The case studies provide evidence that these partnerships can effectively function in order to combat growing concerns. The chapter discussed some of the other limitations of cyber PPPs based on privacy issues and trust and control of operations.

Furthermore, both of these chapters explored the operational diagram of cyber PPPs. These would serve seven major purposes (also portrayed in figure 3.1/Appendix 1), by the manner in which it functions [105]:

1) Regulate suppliers (Telecommunications companies, software suppliers, Internet Service providers (ISP's)) and users;
2) Inspect and enforce compliance from these suppliers and users;
3) Provide detection from threats and behaviors that jeopardize security;
4) Protect individual privacies and liberties of users and suppliers;
5) Respond to, and recover from, threats through information sharing;
6) Promote international collaboration with other organizations and countries in order to increase security and stop cybercrimes on broad scales; and

[105] "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models", Intelligence and National Security Alliance, November 2009. p.9-11
http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

7) Promote US government collaboration and information sharing

These functions are vital as these partnerships can become a major tool to developing and increasing stronger and more efficient cybersecurity systems. These partnerships could have potentially prevented or mitigated the cybercrimes against Sony, Target, Citigroup, JP Morgan Chase, and OPM.

Unfortunately, there are limitations to these cyber PPPs, some of which were mentioned in previous chapters. However, the most striking limitation of these cyber partnerships stems from the lack of harmonization in cross-border enforcement and laws. This issue is key as a strong international cybersecurity regime will require the development of harmonized laws and standardization of certain procedures in order to develop and maintain cybersecurity systems. Cavelty describes the issue in her paper when she wrote, "One key issue for all states is the harmonization of law to facilitate the prosecution of perpetrators of cybercrime. Cybercrime is considered a menace to the economic prosperity and social stability of all states that are plugged into the global information infrastructure. All states therefore have an interest in working together to devise an international regime that will ensure the reliability and survivability of information networks."[106] The question becomes twofold: What are the current status of international cyber laws that govern security issues? And what is lacking in these international and domestic laws that is inhibiting the development of PPPs as a measure for enhancing cybersecurity?

The following chapter will address these questions by analyzing existing international laws and cyber initiatives. It will address the differences on a national basis

[106] Myriam Dunn Cavelty, "Critical information infrastructure: vulnerabilities, threats and responses". *Disarmament Forum.* 2007. p.20

with interwoven themes that convey cooperative limitations and identify some solutions that may enhance the development of harmonized cyber laws and PPPs in order to effectively increase cybersecurity on a global scale.

Literature Review

The following section will review some of the existing literature on cyber law. This section will be separated based on national laws as well as international governing bodies that have created specific laws for cyberspace. Cyber laws vary from country to country and it is important to analyze legal texts as well as other related documents in order to encompass a broad perspective of cyber laws and initiatives. Lastly, the legal world is complicated and documents are extensive with in-depth language. The purpose of this chapter is to focus on broad cyber laws and initiatives that have been passed and events that have occurred, along with the common themes among them. There will be many documents that extend beyond the scope of this study. Therefore, full versions of these documents will be available (through their links) in the bibliography for further study.

International Governing Bodies

The three international governing bodies with the most literature on the subject are the North Atlantic Treaty Organization (NATO), the United Nations (UN), and European Union (EU). NATO was signed into effect in 1949 as a military and political alliance to promote democratic values and military alliances with the hopes of serving a deterrent function for military conflicts. NATO currently has twenty-eight member countries in the alliance to promote collective security.[107] Until the last decade most of

[107] *What is NATO?,* NATO, Accessed June 5th, 2016. http://www.nato.int/nato-welcome/index.html

the measures taken by the alliance have dealt mostly with physical security issues. The laws and principles that make up the foundation of NATO are based upon the previous century of world affairs and conflict. However, all of this has changed with the advent of cyberspace.

The last decade has caused a rise in the legal developments that govern cybersecurity. NATO has recognized the need for cyber initiatives based on recent developments. In 2012, NATO released the *National Cyber Security Framework Manual.* This was an extensive report with ideas and suggestions on how to better international cybersecurity. One of its main themes was the need for "a National Cyber Security (NCS) Strategy, [which] needs to consider the 'three dimensions' of activity: the governmental, the national (or societal) and the international."[108] The need for multilateral cooperation became a recognized requirement for the international alliance as cyber issues threaten the security of all members of the alliance. The report had many elements but the need for cooperation was a strong theme throughout the document. Building on this theme, in 2014, NATO peer-reviewed another series of the Tallinn Papers. The Tallinn Paper No. 5 was a special issue of the NATO Cooperative Cyber Defence Centre of Excellence of Tallinn, Estonia (CCDCOE). This paper discussed the reapplications of customary international law in a cyber context and the problems that result from interpretation of existing laws and norms in this new context.[109] NATO in this peer-reviewed article

[108] Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012. Page 30. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
[109] Michael Schmitt and Liis Vihul,. "The Nature of International Law Cyber Norms." The Tallinn Papers, A NATO CCDCOE Publication on Strategic Cyber Security. 2014. Page 28. https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf

conveyed the need for a more coherent cyber law, as the current status of the laws and policies were too ambiguous.

In 2014, The Wales Summit Declaration, a statement released by the Heads of State of certain governments participating in the meeting of the North Atlantic Council, solidified the way in which cybersecurity is viewed from the perspective of NATO. The statement read:

> As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.[110]

This statement is vital, as it has come to define the way in which NATO perceives cybercrimes. NATO now recognizes certain cybercrimes as an Article Five violation. Article Five is the cornerstone principle of the alliance that affirms an attack against one member is considered an attack against the alliance, thus, it will elicit a collective response.[111] For example, acts of cyber terrorism, if severe enough against particular

---

[110] *Wales Summit Declaration*: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. NATO. 31 Jul. 2015, Accessed June 9th, 2016 http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[111] *The North Atlantic Treaty. Washington DC, April 4th 1949*. Accessed June 10th, 2016 http://www.nato.int/cps/en/natolive/official_texts_17120.htm

targets, can become grounds for Article Five retaliation.

The second governing body that has major influence on cyber law in the international sphere is the United Nations (UN). The UN is an international body, founded in 1945, that promotes peace, security, human rights, equality, and a broad host of strong values. The UN is also an international forum for its 193 member states to come together and tackle these issues as a cohesive unit.[112] The UN has also become an international body for the development of cyber laws and initiatives to combat the growing threats of cybercrimes in the current world environment. The UN works closely with NATO in many of its security principles as participants usually share a dual membership between NATO and the UN. In the last decade, the UN has increased its cybersecurity strategy and legal writings. The first major example came in 2011. The idea of cyber norms emerged as a foundational theme for UN activities. Tim Maurer, an expert in the cyber field, published a study, titled *Cyber Norm Emergence at the United Nation– An Analysis of the UN's Activities Regarding Cyber-security*, through the Belfer Center for Science and International affairs, at the Harvard Kennedy School.[113] The study explained that, "In sum, the literature on soft and hard law shows that soft law plays an important role in international relations. It can lead to an international treaty or exist in addition to a treaty…Understanding which norms will become law (soft law as well as hard law) and how, exactly, compliance with those laws comes about would seem, again, to be a crucial topic of inquiry that lies at the nexus of law and international relations (IR)

[112] *Overview*. The United Nations. 2016. http://www.un.org/en/sections/about-un/overview/index.html
[113] Tim Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?," Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

because these legal rules guide and determine the political actors' behavior."[114] In other words, understanding the laws and compliance with those laws is difficult process. In 2011, the UN began changing their policies and activities to combat these growing cyber threats.

In 2013, the UN General Assembly held a forum to discuss a report by a Group of Governmental Experts on developments in the Field of Information and Telecommunications in the Context of International Security (herein known as the Group). The report stated:

> [T]he Group's conclusion that international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible Information and Communication Technologies (ICT) environment. The Group also concluded that State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory; States must meet their international obligations regarding internationally wrongful acts attributable to them.[115]

The report became an internationally acclaimed document for the need to develop cyber laws.

Over the next two years the UN became set on developing cyber laws and norms. Another working group met in early 2015 in order to address these issues. A Politico article highlighted the main tasks of the working group. Those tasks included outlining international laws in cyberspace during war and peacetimes and the application of humanitarian principles.[116] The Group followed up with another report in July of 2015,

---

[114] Ibid. Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?." P. 14

[115] "Group of Governmental Experts on developments in the Field of Information and Telecommunications in the Context of International Security." United Nations Generally Assembly. June 24th, 2013. Page 2. https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf

[116] Joseph Marks. *U.S. makes new push for global rules in cyberspace*. Politico, May 5th, 2016. Accessed June 18th 2016. http://www.politico.com/story/2015/05/us-makes-new-push-for-global-rules-in-cyberspace-

which called for the states to work through UN principles in order to incorporate and develop cyber laws into the international community. The Group emphasized the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs. While recognizing the need for further study, the Group noted the inherent right to take measures consistent with international law and as recognized in the Charter. The Group also noted that "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction."[117] The United Nations has set the tone for the development of cyber laws through their underlying principles that can be traced back to the mid 20th century. However, thus far, the UN has mostly produced reports rather than adopting these laws and principles into their doctrine.

The last international governing body to mention is the European Union (EU). The history of the EU can be traced back to the 1950s. The EU as it is recognized today came into place in the 1990s. It has twenty-eight European members and serves as the forum that attempts to sustain and develop political and economic prosperity and security for its members.[118] The EU has one of the most comprehensive cyber strategies and legal basis. This is partly due to the fact that it is a much smaller organization than the UN or NATO. But its cyber doctrine intertwines existing laws and then adapts them to cyber laws. For example, the doctrine has sections containing privacy, responsibility, freedom of expression, commerce, foreign affairs, and a multitude of other areas. The shared

---

117632

[117] "Group of Governmental Experts on developments in the Field of Information and Telecommunications in the Context of International Security." United Nations Generally Assembly. July 22nd, 2015. Page 3. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[118] *The EU in Brief*. European Union. Accessed June 12th 2016, http://europa.eu/about-eu/basic-information/about/index_en.htm

responsibility element is interesting because it sets a forum for legal foundations of sharing security issues and working as a cohesive cyber defense force. "All relevant actors, whether public authorities, the private sector or individual citizens, need to recognize this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity."[119] In other words, responsibility of cybersecurity should be dispersed across all actors from a legal sense. The EU's cyber law doctrine is a solid foundation for furthering developing laws.

Countries

For the purposes of this thesis, the United States (US), is the only country specifically chosen for review of its literature. The reason for doing so is that the US is a world leader in cybersecurity law and initiatives, and there are simply too many countries to sift through in this thesis.[120]

The US has a comprehensive set of documents dealing with cyber law and cyber initiatives. Multiple agencies and branches of government have influence in producing cyber laws and strategies. Over the last decade, the frequency of these documents have increased and annually, the president produces a cybersecurity strategy and goals for the upcoming year. In 2009, President Obama signed into effect the Comprehensive National Cybersecurity Initiative (CNCI), which set the forum for developing future cyber laws. This initiatives set forth twelve major goals to increase cybersecurity in the public

[119] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission: High Representative Of The European Union For Foreign Affairs And Security Policy." European Union July 2nd, 2013. Accessed June 15th, 2016. p.4 https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[120] However, the most updated versions of available Cyber Strategies, most contain corresponding cyber law developments, is available via the CCDCOE link in the bibliography.

sector.[121] A few years later in 2013, President Obama signed an Executive Order into effect. The goal of this Executive Order was to achieve a variety of goals. These included developing a framework for information sharing, policy coordination, and creating a Congressional Cybersecurity Act.[122]

Once again in 2015 President Obama stressed the need for enhanced cybersecurity. In the 2015, National Security Strategy, there was a section on cybersecurity.

> Drawing on the voluntary cybersecurity framework, we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure…Globally, cybersecurity requires that long-standing norms of international behavior—to include protection of intellectual property, online freedom, and respect for civilian infrastructure—be upheld, and the Internet be managed as a shared responsibility between states and the private sector with civil society and Internet users as key stakeholders.[123]

This strategy brief is vital because it portrays the shift in the focus to enhancing and developing international laws for cyberspace. In addition, a few months later, Congress passed the Cybersecurity Information Sharing act. The main purpose of this act is to develop a framework for cyber information sharing in order to combat growing cyber threats. This law establishes a forum and application for developing cyber law through information sharing to enhance security.[124]

The last interesting piece about the U.S. cyber law developments is that specific

---

[121] *The Comprehensive National Cybersecurity Initiative*. Foreign Policy. The White House Page 2. Date Accessed June 20th, 2016. https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

[122] President Obama, *Executive Order – Improving Critical Infrastructure Cybersecurity*. The White House, Office of the Press Secretary. February 12th, 2013. Accessed June 20th, 2016. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[123] President Obama. National Security Strategy. February 2015. pp. 12-13 https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

[124] Senate, *Cybersecurity Information Sharing Act 2015*. 114th Congress, 1st session, 2015, S.754, Accessed June 21st 2016 , https://www.congress.gov/bill/114th-congress/senate-bill/754/text

agencies produce their own strategies and reports. These reports have been increasing as well in the last decade. Also, in 2015 the Department of Defense (DOD) released a cyber strategy. The document established strategic goals for enhancing cybersecurity and cyber law.[125] The strategy represents the fact that in the last few years attention has turned to cybersecurity and the advent of developing security and laws surround cyberspace.

Issues for cyber partnerships because of the current status of cyber laws

The number of cyberspace documents is increasing, but so too has the need for established laws. In addition, the need for information sharing, the development of public-private partnerships, and the need for cohesive action has been recognized by many of these international bodies and countries. However, there are still many issues with international cyber laws that are inhibiting the development of effective partnerships for information sharing and enhanced cybersecurity. These issues include the lack of a framework for the development of these laws, transnational development of legal structures, major privacy concerns, and trust issues. The following section will explore these issues as the lack of legal foundations play into the expansion of these issues. Solutions will also be presented in order to provide some foundational bases to correct these issues.

Lacking Framework

The international forum lacks a framework for the development and application of laws. The laws must be developed as the basis for these PPPs. However, there is no concrete forum in which these issues can be discussed. National law making bodies are currently the main law writing bodies. Countries are not as likely to follow laws set by

[125] The DOD Cyber Strategy. April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

organizations such as the UN, NATO, and the EU. There is no forum for the development of these international laws. Thus, many of these partnerships lack the framework to be developed. A brief published by the Brent Scowcroft Center on International Security discusses this issue. The brief discusses the "interoperability" of different national forces that make up NATO response teams but points out the lack of a cyber framework which in turn creates significant vulnerabilities.[126] In essence the lack of framework available for these cyber PPPs is alarming. PPPs need a strong legal foundation to set the responsibilities of both the public and private entities in the partnership.

The brief also presents a strong solution for this lack of international framework. The brief calls for cyber framework nations, or partnerships with nations for cybersecurity. The key would be letting the nations develop the framework for the PPP, while achieving collective security goals. The authors wrote, "creating 'cyber framework nations' each of which would lead a cyber framework group and support national capabilities including the establishment, transfer, training, and support of necessary cyber capabilities; the United States would be the best cyber framework nation."[127] This is a strong solution because countries such as the U.S. are developing the legal foundations necessary for creating cyber PPPs. The resilience of cyber systems would become stronger if partnerships had a framework to develop in an international forum.

In addition, establishing a legal framework for these partnerships would enable development and research functions of cyber partnerships. An article out of the Maurer

---

[126] Franklin Kramer, Robert Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO.* Atlantic Council, Brent Scowcroft Center on International Security. May 2016. p.4 http://www.atlanticcouncil.org/publications/issue-briefs/cyber-extended-deterrence-and-nato

[127] Ibid. Franklin Kramer, Robert Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO. May 2016* p.6

school of law of Indiana University discusses this idea. The authors wrote, "The strategic objective of strengthening cybersecurity through technology means law has different functions under this approach, namely facilitating development of full-spectrum cyber capabilities (e.g., through research and development programs and cybersecurity workforce enhancement efforts) and regulating the use of such capabilities."[128] The authors are referencing NATO in their article, but the solution is useful. A legal framework for cyber partnerships would allow the large scale development of programs that can sustain cybersecurity and work efficiently to share information.

Transnational Developments of Legal Structures

The next common theme currently thwarting the development of cyber PPPs is differing legal structures at the national level. These cross-border legal battles are preventing partnerships from functioning effectively across borders. Laws are subject to national governance. Both private and public entities operating overseas are subject to the national laws and initiatives of that country. This creates significant issues for sharing information across borders. This concept is discussed in an article out of the Center on Law and Security at NYU Law. "Efforts to enhance cross-border law enforcement cooperation have been hindered by conflicting laws and policies. In particular, cross-border data transfer restrictions greatly limit international efforts to detect and thwart cyberattacks because international companies must comply with multiple and sometimes conflicting local, national, or supranational data protection laws."[129] In other words, a key

[128] David P. Fidler; Richard Pregent; and Alex Vandurme. "NATO, Cyber Defense, and International Law" (2013). Articles by Maurer School of Law Faculty. Paper 1672. p.21
http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub
[129] Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation". October 2014. The Center on Law and Security/NYU School of Law. p.8
http://www.lawandsecurity.org/portals/0/documents/cybersecurity.partnerships.pdf

function of these PPPs, the rapid sharing of information is limited because of differing national legal structures.

For example, many European countries have ruled that many American countries with operations abroad, are subject to the rules and laws of the countries in which they operate. As one could imagine, companies such as Google, Apple, Facebook, large financial companies, and many others encounter these issues on a daily basis. The issues become exacerbated when the sharing of information is required to combat cybercrimes as demonstrated in two court cases, one involving Google and one involving Facebook. In 2014 the European Court of Justice:

> [I]nterpreted Google's responsibility under European Union data protection laws regarding its online search engine broadly, finding that Google: (1) was subject to Spanish data protection law; (2) was obligated to delete web search results that link to web pages containing accurate but outdated information regarding a person; and (3) upon an individual's request invoking her 'right to be forgotten,' also must delete search results linking to even truthful information about a person that is prejudicial or that she wishes to be 'forgotten' over time. Likewise, in February 2014, the Higher Court of Berlin ruled that Facebook was required to comply with German data protection laws even though Facebook processes German user data at its European headquarters in Ireland.[130]

The subjectivity of national courts jeopardizes the effectiveness and development of cyber PPPs.

A solution to this issue will be standardizing laws at the international level. This would also standardize judicial cooperation to establish similar laws across borders. This could be done through a central international governing body or through the development of similar goals through legal documents. An article from the World Economic Forum discusses this solution. The article suggests that "public and private sectors should seek to

[130] Ibid. Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014. p.8

promote greater global adherence to, and coordination of, the rule of law relating to cybercrime" by efforts such as "ameliorating judicial cooperation in order for mutual legal assistance to be more efficient" and by encouraging "law enforcement authorities and the private sector to join existing public-private cooperation platforms and to enhance and increase coordination between them."[131] The harmonization of cyber laws across borders will help enhance cybersecurity on a global scale.

Privacy Concerns

The next issue that is a major concern and has caused the lack of functioning PPPs is privacy. Many argue that privacy is a major concern for these cyber PPPs. Private companies feel vulnerable if their information is accessible by public entities. This has been evident in the news lately. The case of the Federal Bureau of Investigations and Apple and many other privacy concerns have put cyber partnerships in jeopardy. As aforementioned in chapter two, Congressman Bobby Scott addressed this issue in a 2012 House of Representatives Hearing. He said, "I note concern about proposals to expand the ability of private companies to share information with government and ultimately with law enforcement for the purpose of protecting against cybersecurity threats. If we allow vastly overbroad sharing of information, we actually may undermine the very privacy rights which should be at the forefront of our concern."[132] This statement portrays the concern that information sharing can open the door to privacy issues.

There is a lack of legislation as to how information technology and personal

[131] "Recommendations for Public-Private Partnership Against Cybercrime." World Economic Forum. January 2016. p.7, http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf
[132] House. Judiciary Committee. *Cyber Security: Protecting America's New Frontier,* 112th Cong., 1st sess. H. Rept. 112–80. November 15th 2011. Accessed February 25th 2016. p.5

information should be considered if it is accessible in cyberspace. However, it is possible for information to be shared effectively without privacy violations. A strong example of how information sharing can be functional without violating privacy comes from the economic sector. The Information Sharing Analysis Centers (ISACs) provide an "approach to information-sharing that focuses on identifying information requirements for sectors, and organizations within sectors, and building the capacity of these existing information sharing mechanisms…in contrast, a top-down, government-centric approach is unlikely to be able to react with the agility necessary to deal with rapidly evolving threats and attacks."[133] Establishing laws to develop ISACs for partnerships will be key to solving the privacy issues attendant to cyberspace.

Trust and Transparency

The last major legal area lacking from international cyber law is the trust and transparency factor. Many private entities feel that working with the government is a one-way relationship. As the article from the Center on Law and Security at NYU Law states, "the government accepts information that companies share, but is not always capable of rendering tangible assistance in return."[134] The other issue is transparency. Private entities feel as though if anything goes wrong, the blame and accountability will fall on them as they have no idea what happens to the information shared. It can become buried under classification levels. However, to overcome this issue the government should become more transparent about their operations and systems. Assurances can be

[133] Center for Democracy and Technology. "Improving our Nation's Cybersecurity through the public-private partnership.". March 8th, 2011. Page 3.
https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf
[134] Judith Germano, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014. p.3
http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

established by writing laws, granting private entities access to certain cyber systems and technologies.

Collaboration for the Future – Budapest Convention on Cybercrime

There are many issues that cyber partnerships. Collaboration will be critical in order to detect, protect, and respond to cybercrimes. This concept of working together will be crucial to developing successful public-private partnerships. As previously mentioned, a few of the persisting issues to developing partnerships on both the domestic and international level are the lack of an international framework and the lack of consistent legal structures across international borders for investigating, fighting, and prosecuting against cybercrimes. However, there is a positive outlook for the future. The Budapest Convention on Cybercrime (herein known as the Budapest Convention) is a strong platform that has attempted to harmonize actions against cybercrime.

The Budapest Convention was established in 2001 by the Committee of Ministers of the Council of Europe.[135] It was established as an international treaty for countries to sign and ratify. In 2004, there was only five ratifications, but the treaty has gained international recognition and significance.[136] As of 2016, there is a total of fifty-four signatories to the treaty, with forty-nine of those nations ratifying the treaty and adapting the measures of the treaty.[137]

---

[135] "Explanatory Report to the Convention on Cybercrime." Council of Europe. European Treaty Series – No. 185. Budapest 2001. P.1 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

[136] "Charts of Signatures and Ratifications of Treaty 185". Council of Europe. August, 14th 2016. Date Accessed: August 14th 2016. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=JFzJKAup

[137] Ibid. "Charts of Signatures and Ratifications of Treaty 185". Council of Europe.

The Budapest Convention has three major goals aimed at reducing cybercrimes on both the domestic and international levels. The goals, stated in the Council of Europe's Explanatory report, include, "harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime, providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form, (and) setting up a fast and effective regime of international co-operation."[138] These goals provide directives for individual nations to fight cybercrime domestically and collaborate on the international level with other countries of the treaty.

In addition, the treaty separates domestic and international measures. Chapter two of the treaty determines the common conditions and safeguards and develops procedural powers for jurisdictional provisions, real-time collection of data, search and seizure of computer data, preservation of stored data, and a few other measures.[139] These measures provide nations with domestic enforcement, investigative techniques, and jurisdictional power in order to deal with cybercrimes within their borders. Harmonizing these best-practice techniques is crucial in order to boost cybersecurity and enhance the capabilities of individual nations. Chapter three of the treaty covers mutual assistance, 24/7 network sharing for speedy assistance, and extradition rules.

> It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case

[138] "Explanatory Report to the Convention on Cybercrime." Council of Europe. European Treaty Series – No. 185. Budapest 2001. P.4. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

[139] Ibid. "Explanatory Report to the Convention on Cybercrime." Council of Europe. P.4.

> the existing arrangements also apply to assistance under this Convention… (and) contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Parties.[140]

These measures provide countries with the ability to share information and stop cybercrimes across international borders. This function of the treaty is essential as cyberspace is an extensive domain without physical borders.

The Budapest Convention was the first international framework developed for countries to collaborate and fight cybercrimes. Although, the parties are only state actors, this was an important step for the advancement cybersecurity measures, while simultaneously increasing legal and jurisdictional provisions among, what is now, fifty nations. The Budapest Convention in collaboration with public-private partnerships can be vital to enhancing cybersecurity for both the public and private sector as well as on domestic and international levels.

Conclusion of this Chapter

In conclusion, cyber law is complicated. It becomes even more complicated on an international scale through numerous governing bodies, nations, and institutions. There is no world government or world leading institution that governs and develops cyber war. Laws and Governance are made up of a multilateral network of public and private entities. Two questions were asked in the introduction: What are the current status of international cyber laws that govern security issues? And what is lacking in these international and domestic laws that is inhibiting the development of PPPs as a means of enhancing cybersecurity? Both of these questions were answered. This chapter took the

[140] Ibid. "Explanatory Report to the Convention on Cybercrime." Council of Europe. P.4.

reader through existing cyber laws and initiatives as well as discussed factors inhibiting the development of PPPs. The chapter also provided some solutions to overcoming these issues. Cyberspace has become the new reality and without concrete PPPs, individuals, private, and public entities all become at risk to cybercrimes.

Conclusion

There is no doubt that security threats are on the rise. The accessibility of cyber networks has enabled the ability of state and non-state actors to have an impact on the global level. Threats are now imminent and can come from all enemies. Cyberspace has enabled those with less capabilities to play a larger role in foreign affairs and daily activities. There is also no doubt that the world is behind on responding to cybercrimes and cyber threats. To put it simply, there is just too much ground to cover for both the public and private sector. Civilian and military systems are vulnerable to all types of cybercrimes, thus, making an attack or cyber-related incident looming in the near future. The previous attacks on Sony, Target, JP Morgan Chase, Citigroup, OPM, and many other public and private companies are alarming as it appears the attacks are becoming vast and intricate, leaving more people and groups in the wake of destruction. These case studies indicate that if nothing is done to prevent and respond to these cybercrimes, the damage will keep increasing. Maybe even escalating to a point of no return or a massive failure of civilian or military cyber systems. The problem posed in the introduction was what tool could be utilized to prevent, detect, and respond to these cybercrimes?

The answer is the development of cyber public-private partnerships. These PPPs could be a major tool in order to combat the growing rate and threat of cybercrimes. The PPPs would enhance overall cybersecurity of both military and civilian systems by increasing protection and detection, as well as decreasing the response time to response to cybercrimes. As evidently portrayed the PPPs achieve these goals by regulating suppliers, enforcing compliance, providing detection security, protecting individual liberties, response and recovery through information sharing, promoting international

collaboration, and promoting United States Government information sharing and collaboration.[141] These functions are key to making PPPs an effective tool to enhance cybersecurity. The case studies discussed conveyed the viability of the development of these PPPs. Sony, Target, Citigroup, JP Morgan Chase, and OPM are just a few examples of public and private agencies that have become victims to these cybercrimes.

And the mountain to climb is steep if the world is to overcome these obstacles. There are currently a significant number of limitations preventing the development of cyber PPPs. There are privacy concerns, trust and control issues, information sharing issues, and cross-border data and information sharing problems. In addition, the existing legal system has not been developed to support cyber PPPs, as currently there is still only a small framework developed to discuss and create legal documents to combat the issues at hand. These concerns are terrifying as the cyber domain makes capabilities and power asymmetrical. In other words, one needs less capabilities to have a large impact.

However, there is hope. PPPs can be an effective tool to enhance cybersecurity. In addition, the recognition of cybersecurity needs by state and non-state actors such as the US, NATO, UN, EU and many other public agencies and private corporations shows that there is a will to combat cybercrimes. The world is at an interesting point. Cyberspace is a new domain that changes faster than it can be understood. However, with the adaption and development of cyber PPPs, the world can get a jumpstart on combating cybercrimes and bolstering cybersecurity on a global basis.

---

[141] "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models", Intelligence and National Security Alliance, November 2009. http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

References

Appendix 1: Figures

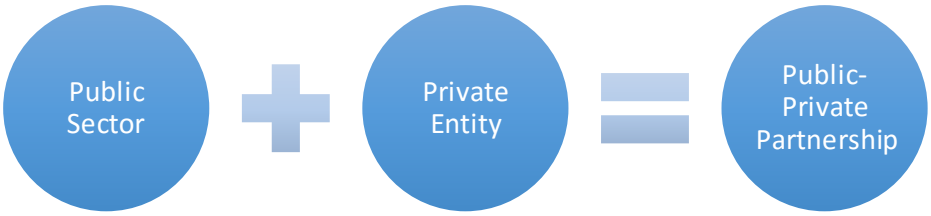

Figure 1.1: Public-Private Partnership Structure

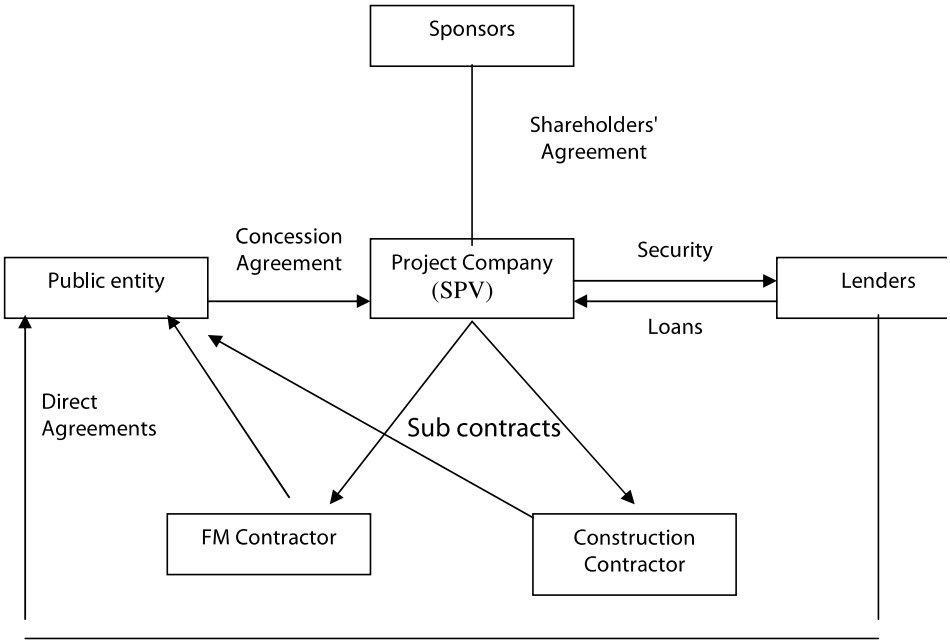

Figure 1.2: Steps to Developing a Public-Private Partnership [142]

[142] Virginia Tan, Allen & Overy, "Public-Private Partnership (PPP)", Advocates for International Development, June 2012, Page 1
http://www.a4id.org/sites/default/files/files/[A4ID]%20Public-Private%20Partnership.pdf

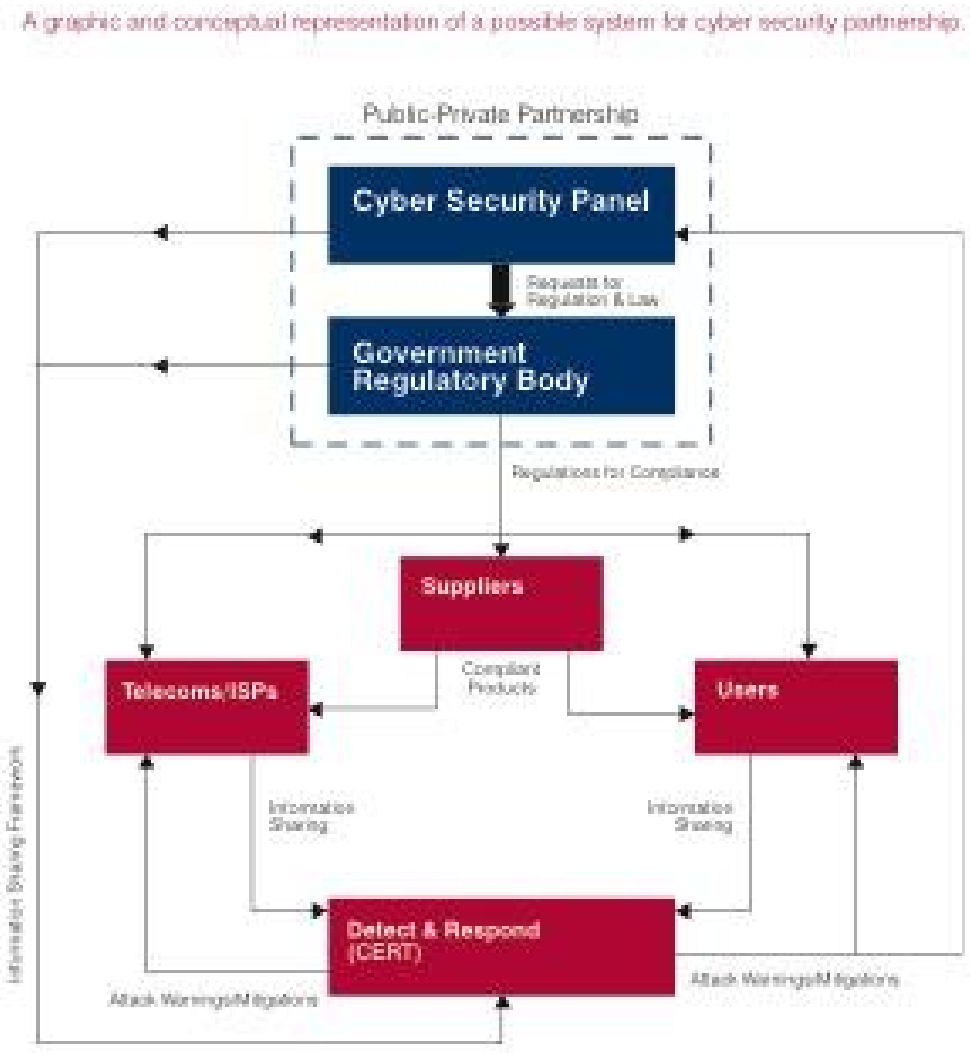

Figure 1.3: Cyber Public-Private Partnership Information Sharing [143]

[143] "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models", Intelligence and National Security Alliance, November 2009. p.9
http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

Picture 1: Key Institutions in the Cybersecurity PPP Landscape

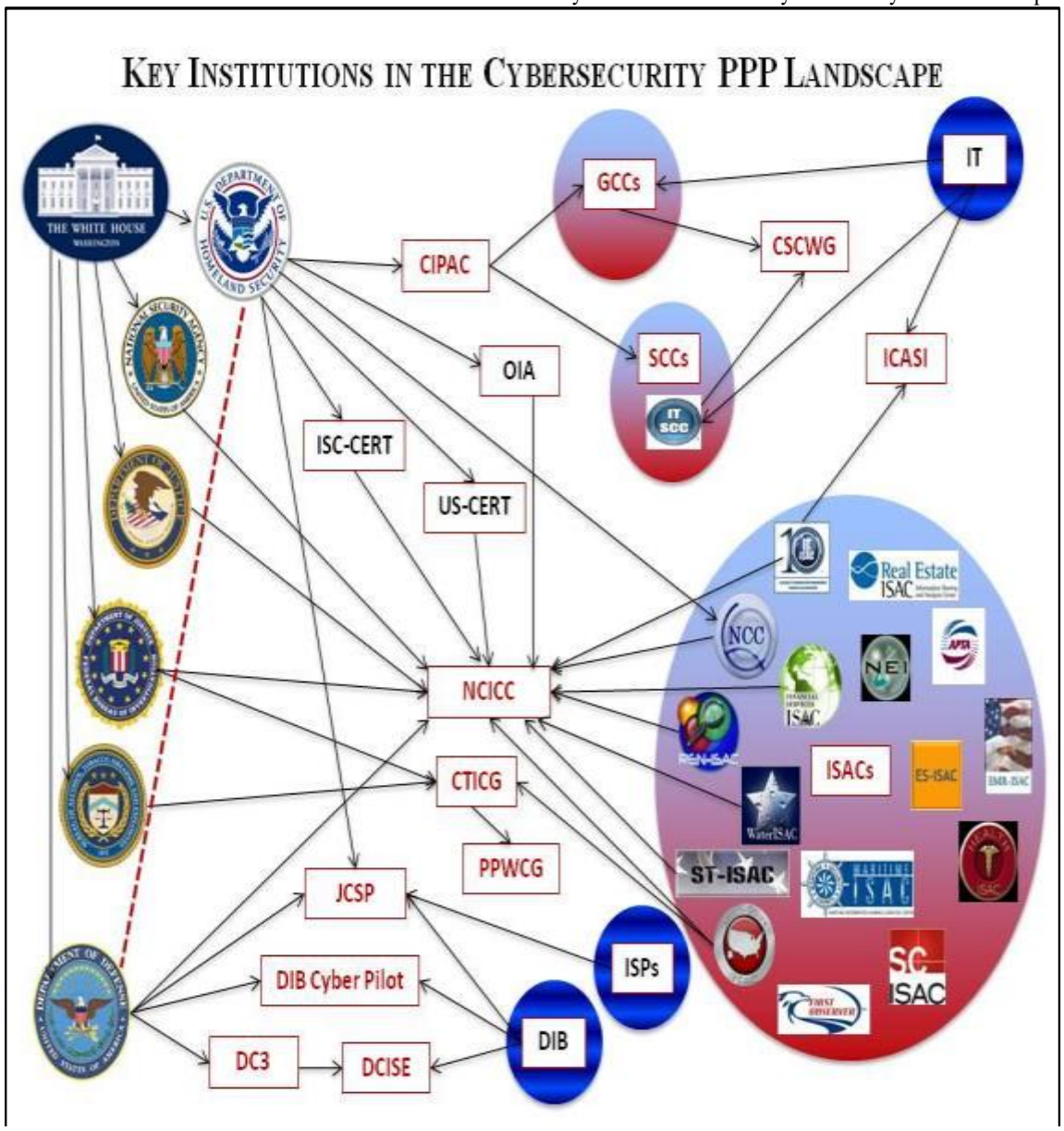

Figure 1.4: Public-Private Partnership Network [144]

[144] Rachael Thomas, "Securing Cyberspace Through Public-Private Partnership", August 2013, p.15 http://csis.org/files/publication/130819_tech_summary.pdf

Appendix 2: Glossary[145]

*Terms taken from the "Explore Terms: A Glossary of Common Cyber Terminology" of the National Initiative for Cybersecurity Careers and Studies (cited in footnote)

- Antispyware software -- program that specializes in detecting and blocking or removing forms of spyware.
- Antivirus software -- a program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents.
- Attack -- an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.
- Authentication -- the process of verifying the identity or other attributes of an entity (user, process, or device).
- Authorization -- a process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.
- Behavior monitoring -- observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.
- Capability -- the means to accomplish a mission, function, or objective.
- Critical infrastructure -- the systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.
- Cyber Infrastructure -- the information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements: Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.
- Cyber Operations -- performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
- Cybercrimes -- criminal offenses committed via the Internet or otherwise aided by various forms of computer technology[146]. These actions include terrorism, hacking, theft, unauthorized access, information dissemination, fraud, scams, copyright of code,

---

[145] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, Feburary10th, 2015, Accessed November 10th, 2015. https://definedterm.com/a/download/document/11128

[146] *Cybercrimes,* FindLaw, Accessed November 10th, 2015 http://criminal.findlaw.com/criminal-charges/cyber-crimes.html

and many other crimes that exist on computer, smartphone, or any digital network

- Cybersecurity -- the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

- Cyberspace – the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

- Data breach -- the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

- Encryption -- the process of transforming plaintext into ciphertext.

- Firewall -- a capability to limit network traffic between networks and/or information systems.

- Hacker -- an unauthorized user who attempts to or gains access to an information system.

- Information and communication(s) technology -- any information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

- Information Security Policy -- an aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

- Information Sharing -- an exchange of data, information, and/or knowledge to manage risks or respond to incidents.

- Malicious code -- program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

- Malware -- software that compromises the operation of a system by performing an unauthorized function or process.

- Mitigation -- the application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

- Network resilience -- the ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands.

- Phishing -- a digital form of social engineering to deceive individuals into providing sensitive information.

- Privacy -- the assurance that the confidentiality of, and access to, certain information

about an entity is protected.

- Response -- the activities that address the short-term, direct effects of an incident and may also support short-term recovery.

- Risk -- the potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.

- Software assurance -- the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

- Spam -- The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

- Spoofing -- Faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system.

- Spyware -- Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

- Threat -- a circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

- Threat agent -- an individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

- Threat assessment -- the product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

- Unauthorized access -- any access that violates the stated security policy.

- Virus -- a computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

- Vulnerability -- a characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Bibliography

"Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models", Intelligence and National Security Alliance, November 2009. http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

Agora, Tripwire, 2014.Date Accessed November 15th, 2015. http://www.tripwire.com/register/agora-case-study/

Arquilla, John and Ronfeldt, David. "Cyberwar is Coming". *In Athena's Camp*. Rand Corporation. 1997, Page 25.

Brown, Frederick. *The Sony Hack: One Year Later*. CNBC. Nov, 24th 2015. Accessed March 8th 2016. http://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html

Butler, Robert; Kramer, Franklin; and Lotrionte, Catherine. *Cyber, Extended Deterrence, and NATO*. Atlantic Council, Brent Scowcroft Center on International Security. May 2016. http://www.atlanticcouncil.org/publications/issue-briefs/cyber-extended-deterrence-and-nato

Carr, Madeline. *Public-Private Partnerships in national cyber-security strategies.* International Affairs, Vol.92 No.1 Chatham House. 2016. Page 57 https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

Cavelty, Myriam Dunn. "Critical information infrastructure: vulnerabilities, threats and responses". *Disarmament Forum*. 2007. http://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2643.pdf

Clarke, Richard A., and Robert K. Knake. *Cyber war*. HarperCollins, 2011.

"Charts of Signatures and Ratifications of Treaty 185". Council of Europe. August, 14th 2016. Date Accessed: August 14th 2016. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=JFzJKAup

Choo, Kim-Kwang Raymond, "The Cyber Threat Landscape: Challenges and Future Research Directions", ScienceDirect: Computers and Security, August 16th 2011, Accessed, 30 Sept. 2015. http://130.18.86.27/faculty/warkentin/SecurityPapers/Newer/Choo2011_C&S30_CyberThreatOverview.pdf

Corrigan, Mary Beth, *Ten Principles for Successful Public/private Partnerships,* Washington, D.C.: Urban Land Institute, 2005.

Crowe, Portia. *JP Morgan fell victim to the largest theft of customer data from a financial institution in U.S. History*. Business Insider. November 10th 2015. Accessed April 17th 2014. http://www.businessinsider.com/jpmorgan-hacked-bank-breach-2015-11

Cybercrimes, FindLaw, Accessed November 10th, 2015 http://criminal.findlaw.com/criminal-charges/cyber-crimes.html

"Cyber Risk-A Global Systemic Threat", A White Paper. DTCC. October 20th,2014. http://www.dtcc.com/news/2014/october/20/cyber-risk.aspx www.dtcc.com/~/media/Files/Downloads/issues/risk/cyber-risk.pdf

"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission: High Representative Of The European Union For Foreign Affairs And Security Policy." European Union July 2nd, 2013. Accessed June 15th, 2016. https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Easton, Mathew. *Living in a Big Data World.* ScienceDirect. Vol 58. January 14th, 2016. Accessed March 3rd, 2016. http://www.sciencedirect.com/science/article/pii/S0747563215303216

"Explanatory Report to the Convention on Cybercrime." Council of Europe. European Treaty Series – No. 185. Budapest 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

Explore Terms: A Glossary of Common Cybersecurity Terminology, National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, Feburary10th, 2015, Accessed November 10th, 2015. https://definedterm.com/a/download/document/11128

Fidler, David P.; Pregent, Richard; and Vandurme, Alex, "NATO, Cyber Defense, and International Law" (2013). Articles by Maurer Faculty. Paper 1672. http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub

Finklea, Kristen and Theohary, Catherine, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement", CRS Report R42547, January 15th, 2015. https://www.fas.org/sgp/crs/misc/R42547.pdf

Germano, Judith, "Cybersecurity Partnerships: A new Era of Public-Private Cooperation", The Center on Law and Security/NYU School of Law, October 2014. http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

Greenberg and Zetter, "Why the OPM Breach is such a Security and Privacy Debacle". Wired June 11th, 2015. Accessed March 3rd, 2015. http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/

"Group of Governmental Experts on developments in the Field of Information and Telecommunications in the Context of International Security." United Nations Generally Assembly. July 22nd, 2015.
http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

"Group of Governmental Experts on developments in the Field of Information and Telecommunications in the Context of International Security." United Nations Generally Assembly. June 24th, 2013.
https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf

"Improving our Nation's Cybersecurity through the public-private partnership", Center for Democracy and Technology March 8th, 2011.
https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf

Istrate, Emilia and Puentes, Robert, "Moving Forward on Public-Private Partnerships: U.S. and International Experience with PPP Units", BROOKINGS-ROCKEFELLER | *Information Sharing*, Department of Homeland Security, Accessed November 10th 2015.
https://www.dhs.gov/topic/cybersecurity-information-sharing

"Keys to Collaboration: Building Effective Public-Private Partnerships" The National Association of State Chief Information Officers (NASCIO) Corporate Leadership Council (CLC)
Transforming Government: Role of Information Technology. May 2006
http://natcapsolutions.org/LASER/LASER_Building-Effective-Public-Private-Partnerships.pdf

Klimburg, Alexander (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012
https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Lynn, William. *Defending a New Domain*. Foreign Affairs, Vol. 89 No. 5 (October 2010). Pages 97-108

Link to National Cyber Strategies of available countries, CCDCOE, most recent versions
https://ccdcoe.org/strategies-policies.html (Footnote 115)

Maniam, Shiva and Rainie, Lee, *Americans feel the tension between privacy and security concerns.* Pew Research Center. February 19th, 2016. Accessed March 4th, 2016.
http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

Marks, Joseph. *U.S. makes new push for global rules in cyberspace.* Politico, May 5th, 2016. Accessed June 18th 2016.
http://www.politico.com/story/2015/05/us-makes-new-push-for-global-rules-in-cyberspace-117632

Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?," Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

McGrath, Maggie. *Target Data Breach Spilled Info On as Many as 70 Million Customers*. Business Insider. Jan. 10th, 2014. Accessed March 10th, 2016. http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#27095bea6bd1

Nakashima, Ellen, "Hacks of OPM databases compromised 22.1 million people, federal authorities say", *Washington Post,* July 9th 2015, Accessed November 8th, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say

"National Security Strategy", White House, February 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

"NATO Cyber Defence." Last Updated June 23rd, 2016. Accessed November 7th 2015. http://www.nato.int/cps/en/natohq/topics_78170.htm

Osborne, Stephen P., *Public-Private Partnerships: Theory and Practice In International Perspective,* London: Routledge, 2000.

Overview. The United Nations. 2016. http://www.un.org/en/sections/about-un/overview/index.html

Perez, Evan. *Obama 'Sony Made a Mistake*. CNN Politics. Dec, 19th 2014. Accessed March 8th, 2016. http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/

Perlroth, Nicole. New York Times. *Target Investigates Breach Involving Credit Card Data*. Dec. 18th, 2013. Accessed April 10th, 2016. http://bits.blogs.nytimes.com/2013/12/18/target-looking-into-security-breach/?hpw&rref=technology&_r=0

President Obama, *Executive Order – Improving Critical Infrastructure Cybersecurity*. The White House, Office of the Press Secretary. February 12th, 2013. Accessed June 20th, 2016. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

President Barack Obama, "Remarks by the President at the Cybersecurity and Consumer Protection Summit", Speech Presented at Cybersecurity and Consumer Protection Summit, Stanford University, Feb. 13, 2015. https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

President Obama. National Security Strategy. February 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

PROJECT ON STATE AND METROPOLITAN INNOVATION | December 2011. http://www.brookings.edu/~/media/research/files/papers/2011/12/08-transportation-istrate-puentes/1208_transportation_istrate_puentes.pdf

Readout of Assistant Attorney General for National Security John P. Carlin's Address at Vanity Fair's 2015 New Establishment Summi, Department of Justice, Press Release. Tuesday, October 6, 2015. Accessed March 3rd, 2016 https://www.justice.gov/opa/pr/readout-assistant-attorney-general-national-security-john-p-carlin-s-address-vanity-fair-s

"Recommendations for Public-Private Partnership Against Cybercrime." World Economic Forum. January 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf

Report to Secretary of the Defense: Public Private Collaboration in the Department of Defense. Defense Business Board. *2012* http://dbb.defense.gov/Portals/35/Documents/Reports/2012/FY12-4_Public_Private_Collaboration_in_the_Department_of_Defense_2012-7.pdf

Rid, Thomas, *Cyber War Will Not Take Place*. Journal of Strategic Studies, Vol. 35 No. 1 (February 2012). Pages 5-32

Schmitt, Michael and Vihul, Liis. "The Nature of International Law Cyber Norms." The Tallinn Papers, A NATO CCD COE Publication on Strategic Cyber Security. 2014 https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf

Selyukh, Anlina. "FBI Chief and Apple's Top Lawyer head into First Encryption Hearing". NPR. March 1, 2016, Accessed April 4th, 2016. http://www.npr.org/sections/thetwo-way/2016/03/01/468599364/fbi-chief-and-apples-top-lawyer-head-into-first-encryption-hearing

Shackelford, Scott. *Protecting Intellectual Property And Privacy In The Digital Age: The Use Of National Cyber security Strategies To Mitigate Cyber Risk*. Chapman Law Review. 2016 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2635035

Smith, Aaron. *Citi: Millions Stolen in May Hack Attack*. CNN Money. June 27th 2011. Accessed April 16th 2016. http://money.cnn.com/2011/06/27/technology/citi_credit_card/

Solomon, Jay, "U.S. Detects Flurry of Iranian Hacking", *The Wall Street Journal*, November 4th 2015, Accessed November 10th, 2015. http://www.wsj.com/articles/u-s-detects-flurry-of-iranian-hacking-1446684754

Soltra Edge: Robust, Open, Free, Soltra, A DTCC and FS-ISAC Company, Accessed November 10th, 2015. http://soltra.com

Stone, John, "Cyber War Will Take Place!", *Journal of Strategic Studies*, Vol.36, No.1, 101-108, November 29th, 2012.

Tan, Virginia, Allen & Overy, "Public-Private Partnership (PPP)", Advocates for International Development, June 2012. http://www.a4id.org/sites/default/files/files/[A4ID]%20Public-Private%20Partnership.pdf

The Comprehensive National Cybersecurity Initiative. Foreign Policy. The White House Page 2. Accessed June 20th, 2016. https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

The DOD Cyber Strategy. April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

The EU in Brief. European Union. Accessed June 12th 2016, http://europa.eu/about-eu/basic-information/about/index_en.htm

The Interview Plot Summary. IMDB. Accessed March 3rd, 2016. *http://www.imdb.com/title/tt2788710/plotsummary*

The North Atlantic Treaty. Washington DC, April 4th 1949. Accessed June 10th, 2016 http://www.nato.int/cps/en/natolive/official_texts_17120.htm

Thomas, Rachael "Securing Cyberspace Through Public-Private Partnership" August 2013 http://csis.org/files/publication/130819_tech_summary.pdf

U.S. Congress. House. Judiciary Committee. *Cyber Security: Protecting America's New Frontier* U.S. Government Printing Office. 112th Cong., 1st sess. H. Rept. 112–80. November 15th 2011. Accessed February 25th 2016. https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg71238/html/CHRG-112hhrg71238.htm

U.S. Congress. Senate. *Cybersecurity Information Sharing Act 2015*. 114th Congress, 1st session, 2015, S.754, Accessed November 7th, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754/text

US-EU Safe Harbor Invalidated: what now?, Proskauer, October 2015. Accessed November 16th, 2015. privacylaw.proskauer.com/2015/10/articles/European-union/us-eu-safe-harbor-invalidated-what-now/

Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. NATO. 31 Jul. 2015 09:05 http://www.nato.int/cps/en/natohq/official_texts_112964.htm

What is NATO?, NATO, Accessed June 5th, 2016. http://www.nato.int/nato-welcome/index.html

Curriculum Vitae

Jake Rogers was born in 1993 in Long Island, New York. Growing up near a large international city, accompanied with extensive travels, sparked his interest in foreign affairs and international relations. He attended Johns Hopkins University. He graduated in the Spring of 2015 with a Bachelor of Arts in Political Science and a minor in Global Environmental Change and Sustainability. During his undergraduate studies, he maintained an interest in foreign affairs and international relations and developed an interest in global security issues. His post-graduate studies have encompassed a wide range of global security studies with a focus in strategic studies. The in-depth research of this thesis process has provided him with a strong knowledge base of cybersecurity concerns. He trusts that his studies will have prepared him for a career in the global security field.